Universidad Politécnica de Madrid

Escuela Técnica Superior de Ingenieros Informáticos

Proyecto fin de carrera

Investigación informática forense basada en Emacs

Autor: José Luis Jerez Guerero
Tutor: Fernando Pérez Costoya

Madrid, Julio 2015

Investigación informática forense basada en Emacs

José Luis Jerez Guerero

Madrid, Julio 2015

Tutor:

Fernando Pérez Costoya (fperez@fi.upm.es)

La composición de este documento se ha realizado con Emacs LaTeX.
Diseño de Oscar Cubo Medina adaptado por José Luis Jerez.

Índice

Capítulo 1: INTRODUCCIÓN

Agradecimientos

Me gustaría agradecer, en primer lugar a mi familia. Los que no están, mis abuelos y mis tíos y los que continúan soportándome, mis padres y hermanos, por empujarme constantemente a realizar el proyecto e inculcarme lo necesario que es ampliar conocimientos para crecer como persona. También por haberme facilitado estudiar en las mejores condiciones posibles, sin reparar en gastos ni esfuerzos en mi educación.

En mi opinión, la vida es un ciclo de `aprendizaje, aplicación y enseñanza`. Los resultados del aprendizaje, así como de la aplicación de los conocimientos adquiridos dependen de la `aptitud` principalmente, sin embargo, la docencia requiere de una `actitud` que no todo el mundo posee en igual medida.

Por ello, también me gustaría agradecer a todos aquellos PROFESORES que siempre recordaré como Rafa Morales, Joaquín Erviti, Jacinto González-Pachón o Marisa Córdoba por nombrar algunos, que en algún momento de mi carrera han contribuido a mi aprendizaje, tanto humano como profesional, y me han mostrado interés y apoyo.

Por supuesto quiero agradecer sus enseñanzas a lo largo de la carrera, quizás, al igual que el resto de PROFESORES más de las que él/ellos mismo/s puede/n imaginar, así como su interés y dedicación en el proyecto al PROFESOR Fernando Pérez, tutor del mismo, que ha resuelto todas mis cuestiones y me ha facilitado las tareas haciendo que parezca fácil una labor que, dentro del día a día de un PROFESOR, no lo es.

De todos ellos, quizás lo más valioso que he aprendido es la correcta actitud a la hora de enseñar y lo complejo que resulta hacerlo bien.

Tampoco puedo olvidar a todos los compañeros con los que he compartido apuntes y largas prácticas.

Y por último, pero no por ello menos importante, me gustaría expresar mi agradecimiento especialmente a una persona, Aurora, por equivocarse al elegirme como compañero en la vida y en el estudio, y por su apoyo incondicional. Si no fuera por su insistencia, es posible que hubiera tardado muchos años más o incluso que nunca hubiera terminado la carrera. Es que es MUY... :)

Resumen ejecutivo

Debido a mi trabajo, me veo involucrado de forma recurrente en proyectos relacionados con algo que se identifica como trabajos de *análisis de seguridad*, si bien su carácter no se limita a labores de análisis, de donde podría decirse que se trata de *trabajos* o *investigaciones* relativas a distintos aspectos del mundo de la seguridad lógica. En algún caso concreto, estos trabajos identificados coloquialmente como *análisis forense* o *informática forense*, me han llevado a actuar como *perito informático forense* designado por una de las partes en *investigaciones privadas*, o como responsable del equipo de peritos en *investigaciones penales*. Sin embargo, en la mayoría de los casos, mi labor está asociada con el perfil de *experto en seguridad* en el entorno empresarial o gubernamental, ya sea desde el campo de la *monitorización y respuesta a incidentes de seguridad* o en proyectos de *hacking ético*.

Llegados a este punto, ya he utilizado varios conceptos que aparentemente se refieren a la misma actividad, pero que, desde mi experiencia, identifico grandes similitudes en el objetivo a alcanzar y enormes diferencias en las metodologías utilizadas en cada caso.

Los conceptos clave identificados en el párrafo inicial son: *análisis de seguridad*, *investigación*, *análisis forense*, *informática forense* y *peritaje informático forense*. Hay otros términos como *hacker ético* que podría tener en cuenta, pero en algún momento hay que establecer un límite.

A priori, todo lo relativo a temas de *seguridad informática*, es muy interesante y llamativo. Sin embargo, hay una gran diferencia entre realizar una *investigación* de una intrusión en un equipo para una empresa que lo que busca es protegerse frente a ataques que pongan en riesgo sus activos y realizar un *peritaje*

informático forense en el que dependiendo del resultado de tu labor hay puestos de trabajo en juego, penalizaciones económicas o incluso pérdida de libertad para alguna persona.
He comentado que, a priori, parece todo muy interesante. Desde el punto de vista de la labor técnica asociada a este tipo de actividades siempre se trata de un reto[1]. Es un trabajo similar a recomponer una fotografía que ha sido troceada, pero con una doble complicación: hay que encontrar los trozos adecuados (pruebas) que se encuentran entremezclados con otros y, en la mayoría de los casos, se desconoce la imagen que conforma dicha fotografía o gran parte de la misma.
En particular, para afrontar los proyectos de *peritaje informático forense* me encontré con que, a pesar de que existen gran cantidad de herramientas e información técnica para realizar un *análisis forense*, el volumen de información relativa a metodologías, buenas prácticas o entandares de actuación para afrontar una *investigación pericial informática forense* entendida desde la globalidad o completitud de la misma, u otras fases de la *investigación forense* no era suficiente, por lo que el resultado del proyecto se cimentaba en los conocimientos técnicos y en el sentido común.
La mayor parte de la documentación que encontré para enfrentar los proyectos estaba desarrollada en Estados Unidos o en otros países europeos, por lo que estaba escrito en inglés. La barrera idiomática es un aspecto que se puede vencer con la formación adecuada, sin embargo, el enfoque de la documentación en general, y en particular los aspectos relativos a la orientación de las actividades relativas a tareas periciales estaba muy orientada a la legislación propia de cada país, lo que la hacía en general inútil por impracticable en España.
En este sentido, planteé el proyecto a partir de esta necesidad que yo mismo había identificado desde hace unos años.
El mayor problema desde mi punto de vista, es a la hora de afrontar una investigación informática que en alguna etapa de la misma se va a *judicializar*. No se trata 'únicamente' de componer la fotografía adecuadamente, sino que hay que hacerlo de forma que el resultado de la misma cumpla con los requisitos exigidos para ser aceptados en un proceso judicial.
Adicionalmente, tenía dudas acerca del alcance y la relación entre los diferentes conceptos clave que enumero al inicio de este apartado. En particular, no tenía claridad acerca del concepto 'forense' fuera de un proceso judicial, así como de la figura de *analista informático forense* frente a la del *perito informático forense* en el contexto de una *investigación informática forense*.
Sin embargo, a raíz de iniciar la preparación de este proyecto fin de carrera en septiembre de 2012, he encontrado que en los últimos años se ha desarrollado bastante documentación, en comparación con lo que encontré cuando inicié el proyecto, acerca de la temática objeto del mismo. En particular, me he apoyado en:

- Libro escrito por Rafael López Rivera. Un perito, mediador y tasador informático y tecnológico español.

    - Peritaje Informático y Tecnológico. Un enfoque teórico-práctico. Tipología - Normativa - Recopilación - Informe - Seguridad.

- Libros escritos por el Prof. Ing. Luis Enrique Arellano González (Ing Informática-Abogado-Lic Criminalística, Director Curso de Informática Forense Facultad Regional Avellaneda en Universidad Tecnológica Nacional de Argentina) y la Prof Ing María Elena Darahuge (Lic en Informática y Enfermería, Ingeniera en Informática, Instructor CCNA. Secretaria Académica Curso de Informática Forense Facultad Regional Avellaneda en Universidad Tecnológica Nacional de Argentina).

    - Manual de informática forense. Prueba indiciaria informático forense. Bases metodológicas: Científica, sistemática, criminalística, tecnológica-pericial y marco legal.

[1] Cuando escribí este apartado no tenía previsto terminar desarrollando un reto forense, por lo que al releer éste me ha parecido una curiosa sincronicidad.

    - Manual de informática forense II. Prueba indiciaria informático forense. Bases teóricas complementarias. Metodología suplementaria: computación móvil (tablet, celulares, iPhone, iPad, iPod, GPS, Mac, imágenes, audio, video, Android, CD, DVD).

- Libro escrito por Ernesto Martínez de Carvajal Hedrich, Técnico Superior Informático, Consultor e-comerce (UAH) y Perito Informático.

    - Informática Forense – 44 casos reales.

- Libros del curso *Computer Hacking Forensic Investigator* desarrollados por International Council of E-Commerce Consultants (EC-Council)

    - Libro: CHFI Courseware Volumen 1
    - Libro: CHFI Courseware Volumen 2
    - Libro: CHFI Courseware Volumen 3
    - Libro: CHFI Courseware Volumen 4

- El artículo "Un forense llevado a juicio"de Juan Luis Garcia Rambla que encontré en la web y que posteriormente ha sido facilitado en formato PDF y licenciado como Creative Commons.

    - Además del texto, en el PFC he trasladado parte del conocimiento que adquirí durante una charla con Juan Antonio Calles y Juan Luis García y el profesor de CHFI durante una RootedCon.

El principal objetivo de este proyecto, tal como se especifica más adelante, es desarrollar una serie de buenas prácticas dentro del ámbito informático forense. Éstas serían la base de una metodología informática forense, para que cualquier persona con los conocimientos técnicos adecuados pueda afrontar una investigación pericial informática forense con garantías de poder afrontar un proceso judicial.
Los objetivos secundarios son:

- Explorar las posibilidades de alinear las buenas prácticas desarrolladas con el uso del editor de textos `Emacs`, y un método de gestión de las actividades conocido como `Getting Things Done` (GTD), utilizando el modo `orgmode` de Emacs.

    - `GTD` se basa en el principio de que una persona necesita borrar de su mente todas las tareas que tiene pendientes guardándolas en un lugar específico. De este modo, se libera a la mente del trabajo de recordar todo lo que hay que hacer, y se puede concentrar en la efectiva realización de aquellas tareas.
    - `ORGMODE` es un modo de edición del editor de texto Emacs mediante el cual se editan documentos jerárquicos en texto plano. Su uso encaja con distintas necesidades, como la creación de notas de cosas por hacer, la planificación de proyectos y programación, entre otros aspectos. Por ejemplo, los elementos to-do (cosas por hacer) pueden disponer de prioridades y fechas de vencimiento, pueden estar subdivididos en subtareas o en listas de verificación, y pueden etiquetarse o darles propiedades. También puede generarse automáticamente una agenda de las entradas de cosas por hacer.

- Facilitar las plantillas de documentación y herramientas que permitan a un perito informático forense abordar una investigación informática forense, siguiendo las buenas prácticas definidas en el presente documento, con garantías de que las tareas realizadas, así como las evidencias presentadas serán aceptadas en un proceso judicial.

- Explicar las diferencias básicas entre el concepto sobreentendido socialmente como *análisis forense* y el *peritaje informático forense*.

No es objetivo de este proyecto desarrollar herramientas concretas con objetivos forenses ni una metodología completa de peritaje informático forense.

Origen del proyecto

El Proyecto Fin de Carrera (PFC) "Investigación informática forense basada en Emacs" nace de la motivación personal por conocer en profundidad dos materias, a priori sin ningún tipo de relación, en las que tenía un interés especial desde hacía tiempo y a las que debido al elevado tiempo que se requiere para su auto aprendizaje, no había podido acometer. Las dos materias son:

- Investigación informática forense.
- Emacs.

El reto de aunar en un objetivo concreto ambas materias a la vez que profundizaba en el conocimiento de las mismas es, por tanto, el origen y la motivación del desarrollo del PFC.

Objetivos

Los distintos objetivos que se desea alcanzar con realización a este proyecto son:

Id. Objetivo	Descripción del objetivo
Obj-1	Identificar y explicar las diferencias entre las actividades nombradas como análisis forense y el peritaje forense.
Obj-2	Estudiar las metodologías relativas al ámbito forense y tecnologías existentes para implementar las distintas capacidades del software que se requieren para la gestión de un proyecto forense.
Obj-3	Desarrollar un documento de buenas prácticas forenses basadas en estándares o mejores prácticas reconocidas internacionalmente.
Obj-4	Utilizar Emacs con org-mode y GTD (Get Things Done) para gestionar y ejecutar una investigación informática forense.
Obj-5	Desarrollar la documentación necesaria para facilitar el uso de las tecnologías seleccionadas e identificar los fundamentos del PFC.
Obj-6	Analizar, diseñar e implementar los elementos necesarios que permitan desarrollar una investigación forense basada en el uso de Emacs.
Obj-7	Realizar un planteamiento fácilmente ampliable y reutilizable.
Obj-8	Definir los formatos que tendrán los ficheros tanto de entrada como de salida que manejará el investigador informático forense.
Obj-9	Diseñar los elementos necesarios que permitan a todo tipo de usuarios realizar un investigación de manera sencilla.
Obj-10	Implementar distintos métodos de ejecución que permitan el funcionamiento bajo los principales sistemas operativos de ámbito general sin necesidad de realizar configuraciones previas.

Organización del documento

La organización de los contenidos de este documento sigue la siguiente estructura de ideas:
INTRODUCCIÓN
Descripción del alcance del documento resaltando el propósito y los objetivos de alto nivel que se pretenden alcanzar con la creación de documentación de buenas prácticas y el desarrollo de la aplicación de gestión del proyecto forense.
INVESTIGACIÓN INFORMÁTICA FRENTE A ANÁLISIS INFORMÁTICO

- ¿Por qué lo llaman análisis cuando quieren decir investigación?
- Servicios de seguridad
- El proceso de investigación

INVESTIGACIÓN INFORMÁTICA FORENSE

- Investigación informática forense
- El perito informático
- Principios básicos a seguir
- El informe pericial

ARTEFACTOS Y EVIDENCIAS DIGITALES

- Artefactos
- La evidencia digital
- La cadena de custodia

EMACS

- ¿Por qué Emacs?
- Emacs: Conocimientos mínimos para enfrentar un análisis forense
- Programación literaria

BUENAS PRÁCTICAS FORENSES Y DOCUMENTALES

- Buenas prácticas
- RFC 3227
- ISO/IEC 27037
- UNE 197001:2011

METODOLOGÍA PROPUESTA

- Metodología de investigación digital forense basada en Emacs
- Procesos básicos de una investigación forense

- Herramientas forenses propuestas

`PoC`

- Prueba de concepto
- Entorno de trabajo: Estación forense
- Reto forense UNAM Episodio III

`Conclusiones y líneas futuras`

- Conclusiones
- Líneas futuras

Desarrollo y costes del proyecto fin de carrera

El PFC, como cualquier proyecto, requiere de una serie de recursos de diferentes tipos así como de una serie de elementos relacionados con el proyecto a alto nivel.
Entre estos elementos cabe resaltar la planificación y el seguimiento de la realización del PFC.
La idea inicial era confrontar la planificación inicial con el desarrollo real del proyecto para sacar las conclusiones oportunas, sin embargo, cuando una vez transcurrido más de año y medio vi la gran cantidad de tiempo dedicado al proyecto, decidí dejar de contabilizarlo para que no se convirtiese en un condicionante a la hora de tomar decisiones acerca de si continuar trabajando sobre un tema o acotar el mismo.
Por otro lado, pensaba realiza una clasificación de los medios y recursos que han sido necesarios en el transcurso del proyecto, relacionándolos con un presupuesto simulado teniendo en cuenta los costes directos e indirectos del mismo. En el mismo momento que decidí dejar de contabilizar el tiempo dedicado también decidí no analizar los costes del mismo, por la misma razón antes expresada.
En cuanto a la planificación del proyecto, éste se compone de dos partes claramente diferenciadas. Una primera parte que desarrolla la base de conocimiento, metodológica y de gestión de un proyecto forense. Y en segunda instancia, el desarrollo de los complementos necesarios para la metodología basada en Emacs que permita gestionar un proyecto forense y que sea independiente de plataformas y sistemas operativos.
El planteamiento seleccionado para usar en este proyecto ha sido, de alguna manera, el clásico ciclo de vida en cascada, pasando por las fases de:

- Análisis inicial de tecnologías y metodologías: Comprende el estudio de las tecnologías y metodologías de análisis forense, así como el conjunto de pruebas desarrolladas para comprobar el efecto que tienen la instalación de aplicaciones sobre los distintos sistemas operativos.
- Análisis de requisitos: Fase en la que se ha recopilado los requisitos en función del enunciado propuesto en el PFC.
- Diseño de la solución: Elaborado a partir de los requisitos, teniendo en cuenta que desde el principio se estableció como prioritario utilizar una arquitectura que independizara los distintos componentes.
- Implementación + Pruebas: Proceso de implementación de la metodología propuesta con el conjunto de herramientas desarrolladas para la resolución de un reto forense.

Exordio

El término *forense*

La piedra angular del proyecto.
El calificativo `forense` tiene su origen en el latín *forensis*, que según la RAE significa perteneciente o relativo al foro. El nombre masculino `foro` al que se hace referencia, viene del latín *forum*, que según una de las acepciones de la RAE es, en la antigua Roma, plaza donde se trataban los negocios públicos y donde el pretor celebraba los juicios.
En el antiguo imperio romano, una imputación por crimen suponía presentar el caso ante un grupo de personas notables en el foro. El proceso implicaba que, tanto la persona acusada de haber cometido el crimen, como la persona denunciante, tenían que exponer su versión de los hechos. La argumentación, las pruebas y el comportamiento de cada persona determinaba el veredicto del caso que se juzgaba.
Hoy en día, el calificativo `forense` se asocia a toda disciplina profesional, como medicina, psicología, grafología, biología, genética, informática y otras, que asesore objetivamente y proporcione soporte a la justicia para que se juzgue un delito. En todas las disciplinas se encuentra el denominador común que el significado forense les imprime, y se aplicaría a *quienes estando en posesión de unos conocimientos especializados y por medio de métodos científicos y sistemáticos,/ /analizan las evidencias para proporcionar su opinión experta sobre las cuestiones que se le planteen al respecto*.

Disciplinas forenses y la informática

La Informática Forense es a la Informática, lo que la Medicina Legal a la Medicina.
La medicina legal es una rama de la medicina que determina el origen de las lesiones sufridas por un herido o, especialmente, la causa de la muerte mediante el examen de un cadáver. Estudia los aspectos médicos derivados de la práctica diaria de los tribunales de justicia, donde actúan como peritos. El médico especialista en el área recibe el nombre de médico legista (de latín legis, 'ley') o médico forense.
Un perito (o experto) es una persona reconocida como una fuente confiable de un tema, técnica o habilidad cuya capacidad para juzgar o decidir en forma correcta, justa o inteligente le confiere autoridad y estatus por sus pares o por el público en una materia especifica.
En España, como en la mayoría de países del mundo, la informática forense no es una rama de la informática. En general, en la actualidad, el perito forense es una persona con un conocimiento amplio o aptitud en un área particular del conocimiento informático y que, gracias a su entrenamiento, educación, profesión, trabajos realizados o experiencia, tiene un conocimiento sobre un cierto tema que excede el nivel de conocimiento de una persona común, de manera tal que otros puedan confiar en la opinión del individuo en forma oficial. Sin embargo, carecen de una formación adecuada en distintas disciplinas periciales criminalísticas.
Si bien, dentro del currículum propuesto por ACM e IEEE para Computer Science en 2013 hay un área de conocimiento denominada 'Information Assurance and Security (IAS)', que incluye una 'unidad de conocimiento' dedicada a 'Digital Forensics'.
Parece adecuado plantear la informática forense como una rama de la informática, sin embargo, entiendo que el mismo planteamiento implica una gran complejidad dado el número de múltiples disciplinas que conforman el espectro informático y que aumenta día a día.

Creo que he sufrido un incidente de seguridad

Un usuario común, antes de realizar ninguna acción por su cuenta, debe saber que la información digital es muy frágil y puede desaparecer o manipularse con mucha facilidad.
Ante un incidente informático el usuario dispone de dos alternativas: tomar acciones legales o no hacerlo.

Desde el punto de vista legal, una acción inadecuada puede invalidar una prueba, que es el medio de verificación de las proposiciones que los litigantes formulan en el juicio.
La recomendación para el usuario común es contactar con un abogado experto en nuevas tecnologías, o un perito informático. Éstos profesionales podrán asesorar al usuario acerca de las posibles acciones a realizar dependiendo de su caso y circunstancias.
En el caso en el que no se desee tomar acciones legales pero se desee conocer el origen del incidente, como en casos de acoso, amenazas o espionaje, el usuario debe mantener la calma, reunir toda la información demostrable sobre los hechos reales sucedidos, y acudir inmediatamente con un perito o analista forense.
Como regla general, las acciones a realizar por un usuario con conocimientos mínimos ante un incidente informático deben ser:

- Identificar las fuentes de información digital que podrían ser susceptibles de aportar evidencias.
- No acceder, manipular o inspeccionar estas fuentes antes de contactar con un perito informático. Incluso el visionado de documentos electrónicos, sin modificarlos, podrían contaminar la prueba (e invalidarla en caso de utilizarse en un proceso judicial).
- Identificar con cuidado cuál es el círculo de confianza. En casos relativos a amenazas, espionaje industrial, o similar, el autor de los hechos puede estar más cerca de lo esperado. Si no confía en el personal informático se debe de proceder con especial cuidado.

De nuevo, a costa de ser reiterativo, la recomendación principal es ponerse en contacto con un perito informático para realizar una preservación adecuada de estas fuentes, así como con un abogado experto en nuevas tecnologías en caso de considerarse las acciones judiciales. Esta fase debe hacerse lo antes posible, ya que la información digital recuperable desaparece con la actividad de los ordenadores que la contienen.

Figura 1: Algunos de los libros utilizados como documentación

Capítulo 2: INVESTIGACIÓN INFORMÁTICA FRENTE A ANÁLISIS INFORMÁTICO

¿Por qué lo llaman análisis cuando quieren decir investigación?

Este apartado pude resultar irrelevante en el ámbito en el que se circunscribe. Sin embargo, creo que hablar con propiedad es necesario, y en el entorno informático el lenguaje se utiliza en muchos casos de forma errónea.
En mi opinión, una persona que quiere programar en C, Ruby, Python o cualquier otro lenguaje, lo primero que tiene que hacer es aprender los conceptos básicos y comunes a cualquier lenguaje de programación. Este tipo de aproximación al conocimiento es lo que marca la diferencia entre un programador de Java y un PROGRAMADOR.
La sociedad está muy acostumbrada a 'nombrar el todo por las partes', lo que provoca importantes errores de concepto a la hora de realizar comparaciones.
Una persona que quiera ejercer como investigador informático forense debe de adquirir una serie de conocimientos metodológicos, desde una perspectiva tanto técnica como legal, comunes dentro del ámbito forense digital.
Cuántas veces se escuchan frases como: 'tuvo que hacer un análisis forense del troyano para determinar el impacto en el sistema'. Es muy posible que esta persona, antes de poder iniciar la labor de análisis del troyano propiamente dicha haya tenido que realizar otra serie de labores de recolección y documentación, y que una vez finalizado el análisis haya tenido que implementar algún tipo de medida para paliar el impacto del malware en su organización, lo que de nuevo queda fuera del ámbito del análisis. Por otro lado, seguramente dicho análisis nunca llegará a presentarse en un proceso judicial, por lo que no es correcta la denominación de 'forense'. Es decir, esta persona ha realizado una investigación digital de un malware, en ningún caso es aceptable que se limite a la fase de análisis y mucho menos que se le pueda calificar de forense.
De igual modo pasa con la denominación de muchas aplicaciones que son identificadas como herramientas forenses ¿'dd' es una herramienta forense? Claramente no, aunque un investigador forense digital podría utilizarla durante su labor.
El objetivo de este capítulo es doble:

- Identificar el punto de inflexión que marca la generalización de un trabajo de investigación o su fase de análisis, dentro del ámbito de la seguridad informática, frente a la especialización que supone una investigación informático forense, un análisis informático forense o peritación informática forense.

- Desarrollar las actividades comunes que cualquier INVESTIGADOR INFORMÁTICO debe de conocer y seguir en su trabajo de día a día.

Una persona que *investiga* un escenario informático y tecnológico, en el que existe la sospecha de haberse cometido algún tipo de acción (incidente) en contra de los intereses del propietario o responsable del entorno ¿es un *investigador o analista informático forense*?
La RAE sea muy generalista con la definición de investigador o investigación, sin embargo la acepción de investigar describe como:

1. tr. Indagar para descubrir algo. *Investigar un hecho*.
2. tr. Indagar para aclarar la conducta de ciertas personas sospechosas de actuar ilegalmente. *Se investigó a dos comisarios de Policía.*
3. intr. Realizar actividades intelectuales y experimentales de modo sistemático con el propósito de aumentar los conocimientos sobre una determinada materia. *Investigar SOBRE el cáncer.*

Subjetivamente no es la definición más adecuada para el concepto que tratamos.
Por otro lado, en la RAE no aparece definido el concepto de *analista informático forense* que es el término más comúnmente aceptado o *investigador informático forense*, sin embargo, podemos encontrar la siguiente acepción dentro de la definición de analista:

1. com. Persona que lleva a cabo análisis informáticos.

La RAE define la acepción *informática* asociada el término análisis en la actual definición como:

1. m. Inform. Estudio, mediante técnicas informáticas, de los límites, características y posibles soluciones de un problema al que se aplica un tratamiento por ordenador.

Sin embargo, en la última revisión se ha enmendado la definición y no aparece la acepción cinco (5), referente al ámbito informático.[1] He mandado un correo electrónico a la RAE consultando la razón que les ha llevado a tomar dicha decisión, y la respuesta ha sido la siguiente:

```
En relación con su consulta, le remitimos la siguiente información:

Entendemos que porque se encuentra ya recogida en la acepción general de
la voz.

Reciba un cordial saludo.

_____
Departamento de «Español al día»
Real Academia Española
```

Por lo que se entiende que la acepción explícita al ámbito informático queda eliminada y asociada de forma general a las dos interpretaciones que recogen la acepción general de la voz.

1. m. Distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos.
2. m. Examen que se hace de una obra, de un escrito o de cualquier realidad susceptible de estudio intelectual.

En este punto no podríamos responder a la pregunta planteada. Pero sería factible pensar que una persona (analista informático) que lleva a cabo un estudio, mediante técnicas informáticas, de los límites, características y posibles soluciones de un problema al que se aplica un tratamiento por ordenador, podría dar solución al problema planteado, ¿o no?
¿Y si la intrusión requiere intervención de la justicia? ¿Podría un analista informático ser la figura que resuelve la situación planteada?
En la introducción se ha comentado el término *forense* y su relación con el ámbito de la justicia. Sin embargo, no he podido encontrar una organización solvente que respalde el origen del término *analista informático forense* y su presunta relación con capacidad de resolución de incidentes de seguridad *extrajudiciales*. De alguna forma, todas las referencias a *ciencias forenses* establecen una relación en el ámbito judicial:

- Wikipedia - Cómputo forense: El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

[1] He intentado investigar el motivo de dicha desaparición pero no he encontrado referencias.

- MCKEMMISH, R. (1999) What is forensic computing?[fn:2_2: MCKEMMISH, R. (1999) What is forensic computing? Australian

Institute of Criminology. Issues and Trends in crime and criminal justice. No. 118.]: The computer application based of crime computer has given technology rise to to a new the investigation field of specialisation—forensic computing—which is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable.

- National Center for Forensic Science: Forensics, or forensic science, is the application of science to questions that are of interest to the legal system.
- TuDiscovery: La definición del diccionario de ciencia forense es la aplicación de prácticas científicas dentro del proceso legal.

Por otro lado, en el entorno judicial y legal, este tipo de labores se asocia a la peritación, que según la RAE es:

1. f. Trabajo o estudio que hace un perito.

Siendo, según la RAE, un perito es:

1. adj. Entendido, experimentado, hábil, práctico en una ciencia o arte. U. t. c. s.
2. m. y f. ingeniero técnico.
3. m. y f. Der. Persona que, poseyendo determinados conocimientos científicos, artísticos, técnicos o prácticos, informa, bajo juramento, al juzgador sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia.

En este caso, se define a esta figura como alguien con conocimientos, pero no se desarrolla la definición de la labor que realiza más allá de '*informar*, bajo juramento, *al juzgador* sobre puntos litigiosos en cuanto se relacionan con su especial saber o experiencia.'.
En este punto, las diferentes descripciones contemplarían la casuística de que un *investigador informático* realizase una investigación con su correspondiente análisis informático (siguiendo metodologías adecuadas durante todo el proceso de investigación) pudiendo ser asesorado para ello por un *analista informático*, y que si éste, por alguna razón, no está en disposición de informar al juzgador, se requiera a un perito informático forense que participe en el proceso legal informando al juzgador en función del trabajo realizado por el analista informático.
Tengo entendido que una regla básica que te enseñan en primer año de periodismo es "contrastar la información con diversas fuentes"[2]. Por lo que tras contrastar con otras fuentes, como el diccionario María Moliner, diccionarios de términos informáticos online tanto en español como en inglés, ninguno ha aportado más información o concreción. De hecho, en la actualidad, esta misma casuística se aplica a muchas disciplinas profesionales, en las que se identifica el calificativo de *forense* con personas que poseen unos conocimientos especializados y que, por medio de métodos científicos y sistemáticos, analizan las evidencias para proporcionar su opinión experta sobre las cuestiones que se le planteen al respecto, al margen de que el ámbito sea judicial o extrajudicial.
Por lo tanto, a raíz de los argumentos planteados, creo que, atendiendo a su origen, el adjetivo *forense* está siendo mal utilizado en la actualidad cuando el ámbito de su uso es extrajudicial.
El siguiente párrafo 'Análisis detallado de escenarios resultado de acciones no autorizadas que se producen en los sistemas de información de la empresa, identificación del autor, las causas y el método

[2] http://blogocorp.Blogspot.com.es/2006/11/verificando-datos-contrastando-fuentes.html https://www.meneame.net/c/14297008

empleado.' se corresponde con la oferta de análisis forense de una de las grandes empresas de seguridad españolas, y comete el error semántico que he identificado en la sociedad. En mi modesta opinión, el párrafo anterior especifica de una forma muy acertada el concepto de investigación informática, que se realiza utilizando técnicas y metodologías informáticas que no tienen porque estar relacionadas con aspectos legales.
Es cierto que María E. Darahuge y Luis E. Arellano comentan en su libro[3] que 'la Informática Forense es aplicable tanto en los casos llevados a juicio como en investigaciones particulares solicitadas por empresas u organismos privados', a continuación especifican que cada caso específico debe ser analizado como si fuera a juicio, lo que vuelve a orientar este tipo de tareas hacia los procesos judiciales. En el mismo, los autores enumeran distintas disciplinas informáticas e identifican la informática forense como una especialización crítica ya que es transdisciplinaria en sentido intrínseco (abarca métodos y técnicas de todas las otras disciplinas informáticas) y extrínseco (ya que se nutre de diversas áreas del Derecho y dela Criminalística) al resto de disciplinas informáticas.
En resumen, yo diferenciaría dos tipos de perfiles o niveles de especialización:

- `Investigador informático de seguridad`:
  - Persona con conocimientos informáticos dentro de la rama asociada a la seguridad que, mediante técnicas informáticas y tecnológicas, investiga diferentes aspectos de posibles amenazas concretas (como el análisis de malware), o escenarios resultado de posibles acciones no autorizadas que se producen en sistemas de información de una determinada empresa.
    - Analista informático de seguridad es el profesional de seguridad que desarrolla su actividad íntegramente ligado a tareas de análisis informático dentro del conjunto de tareas a realizar en el proyecto.
- `Investigador informático forense` o `perito informático forense`:
  - Experto informático de seguridad que aplica metodologías informáticas forenses con el fin de participar en un proceso judicial con las máximas garantías de que los argumentos aportados así como las evidencias identificadas cumplen con los requisitos exigidos para que sean aceptados por el juzgador.
    - Analista informático forense es el experto informático que desarrolla su actividad íntegramente durante la fase de análisis en una investigación forense.
  - Este perfil será tratado en detalle en el siguiente capítulo, y el presente proyecto se centra en el desarrollo de la labor del mismo sin entrar en detalle en aspectos técnicos concretos más vinculados con el perfil de investigador informático de seguridad.

Dado el contexto del PFC, se da por sobreentendido que este documento y todo el trabajo realizado se circunscribe al entorno informático. Por lo tanto, eliminaremos dicho adjetivo desde este punto del documento, y sólo se realizarán referencias al mismo en caso de que sea necesario para alguna aclaración, o comparativa con otros ámbitos en los que se realizan actividades similares como análisis médico o perito judicial en falsificaciones de obras de arte.

Servicios de seguridad

Los servicios de seguridad tienen un alcance muy amplio, que se pueden dividir en función de las características del servicio que presta cada uno de ellos:

[3]MANUAL DE INFORMÁTICA FORENSE I. Darahuge, María Elena/Arellano González, Luis E. ISBN-10: 9870112498 Aparición: 10/08/2011 Páginas: 416

- Servicio de seguridad proactiva: Actividades que se dedican a tratar de minimizar el riesgo de que se materialice alguna amenaza que pueda explotar una vulnerabilidad antes de que ésta suceda. Dentro de estas actividades se encuentran las labores de auditoría de seguridad, análisis de malware, test de intrusión, monitorización y correlación de eventos de seguridad, y en general todas las tareas que tratan de prevenir actividades no autorizadas por las políticas de seguridad, ya sean consideradas como delictivas o no.

- Servicio de seguridad reactiva: Actividades asociadas a la respuesta ante un incidente de seguridad.

Es importante tener claro el marco de actuación en cada caso. Para el presente PFC me he centrado en los servicios de seguridad reactiva. Esto es, el incidente es un hecho o se dispone de sospechas, basadas en indicios más o menos claros, para aseverar que se ha cometido un acto en contra de los intereses de la empresa.
El perfil que requiere un investigador experto en seguridad reactiva es de una gran polivalencia, y normalmente requiere de conocimientos de diferentes perfiles expertos en diferentes ámbitos de la seguridad proactiva como analistas de eventos de seguridad, hackers éticos, analistas de malware así como aptitudes en áreas de conocimiento completamente diferentes como la legislación o psicología.
Dentro del ámbito de la seguridad informática, la especialidad de análisis de seguridad puede aportar al profesional experiencias muy satisfactorias, pero también situaciones realmente desconcertantes para una mentalidad matemática. A todo esto se suma una circunstancia difícil de digerir, especialmente para un informático, 'la subjetividad'.
De un proceso de investigación riguroso se espera un resultado objetivo y concreto. Sin embargo, normalmente, a pesar de seguir una metodología concreta que se apoya en procesos, procedimientos y herramientas técnicas en última instancia, y de presentar como resultado un informe técnico, todo el proceso no deja de estar cargado de cierta subjetividad. Es más, en un determinado momento, la decisión final y sus consecuencias será adoptada por alguien (ya sea, por ejemplo, un Director del área de negocio de una empresa o un abogado de la misma) que presenta claras limitaciones técnicas para apreciar lo expuesto en un informe técnico de análisis de seguridad.

¿Es posible que las conclusiones de la investigación haya que defenderlas en un proceso judicial?

Al hilo del párrafo anterior, es crítico para un investigador de seguridad, poder responder desde el inicio de una investigación a la siguiente pregunta:

> ¿Es posible que las conclusiones de la investigación haya que defenderlas en un proceso judicial?

Si bien esta cuestión no altera en ningún caso el objetivo de la investigación y puede parecer poco relevante para iniciar las labores técnicas, es el punto de decisión crítico a la hora de seleccionar la metodología a utilizar.
Si la respuesta a la pregunta anterior es afirmativa, el equipo de investigación de seguridad debe cumplir con una serie de requisitos concretos asociados a sus conocimientos, además de ser consciente de todo lo que implica realizar la labor de perito forense desde el inicio de la investigación hasta la sala donde se desarrollará el proceso judicial.
¿Por qué es importante? En primer lugar, si la investigación forense lo realiza una persona sin la preparación y cualificación adecuada todo el trabajo puede ser inútil, independientemente de la calidad técnica del mismo y de la veracidad de los resultados. En segundo lugar, en el desarrollo del proceso judicial, el tipo de preguntas a las que se enfrente el investigador no serán tan claras y directas como las que en sus labores técnicas contesta habitualmente. En muchas ocasiones éstas serán directamente malintencionadas e incluso retorcidas, y de nuevo, una mala respuesta puede llegar a invalidar judicialmente una buena

labor de investigación forense. En estos momentos es cuando se aprecia lo determinante que es haber realizado correctamente la investigación desde sus inicios. De este modo la duda, la inseguridad y falta de claridad en la respuesta serán infrecuentes. La frustración de 'que estaba casi todo bien' y de que por lo menos 'lo intentamos' será inusual si la metodología aplicada a labor técnica ha sido la adecuada.
Enfrentar adecuadamente y con conocimientos la respuesta afirmativa a la pregunta planteada es el objetivo del presente PFC, y se desarrollará en detalle a partir del siguiente capítulo.
Si la respuesta a la pregunta anterior es negativa, el experto en seguridad debe cumplir con una serie de requisitos concretos asociados a sus conocimientos. Sin embargo, no requiere ser consciente de todo lo que implica realizar la labor de perito forense desde el inicio de la investigación hasta la sala donde se desarrollará el proceso judicial.
Esto no implica que el desarrollo técnico de las tareas realizadas no deban de ser impecables y que el experto no deba de seguir una metodología adecuada, ya que, aunque se determine inicialmente que los resultados de la investigación se tratarán internamente y se descarte tomar acciones legales, enfrentarse a cualquier investigación implica tener que anticipar la posibilidad de llegar a juicio. A menudo, y en función del escenario, es posible que ese hecho no se observe en un principio, pero tal y como se desencadenen los acontecimientos pueda llegar a darse. En estos casos, llegados al punto de inflexión en el que se decide orientar la investigación a un proceso judicial, se deberá de plantear la idoneidad de mantener al experto de seguridad que ha desarrollado el trabajo hasta el momento y la posible necesidad de involucrar a un perito forense.
Por lo tanto, es recomendable que, previo al inicio de la investigación, como experto de seguridad se comunique a los interesados que la recogida y tratamiento posterior de evidencias no va a realizarse atendiendo a los requisitos de un proceso judicial.

Caso hipotético sin desencadenantes judiciales

Expongamos a continuación un caso hipotético y que recoge situaciones que no son inusuales en la realidad y que ilustran la posibilidad de que una investigación técnica no desemboque en un proceso judicial.

```
Se detecta un aumento de tráfico inusual asociado a un servidor de la
DMZ de la empresa y, los primeros datos de la investigación, identifican
que el origen del mismo es un servicio P2P no identificado en la CMDB de
los sistemas de dicha empresa.

En consecuencia se decide continuar con la investigación y averiguar que
está ocurriendo. Se detecta la presencia de un cliente P2P instalado en
el servidor.

En ese momento son múltiples las cuestiones a abordar: ¿por qué el
antivirus no lo ha detectado?, ¿pueden otros servidores estar
afectados?, ¿quién lo instaló?, ¿cuándo se instaló?, ¿qué tipo de
información ha transmitido?, ¿es recomendable eliminarlo?

Sin embargo, en el transcurso de la investigación digital no sólo se
detecta al elemento malicioso, sino que se evidencia una fuga de
información crítica para el negocio.

Se localiza quién ha sido el culpable de la acción maliciosa y a qué
tipo de información ha tenido acceso que evidencia un alto riesgo de
impacto negativo en la imagen de la empresa. La información analizada
```

```
indica que se podría tratar de un grupo de lammers o script-kiddies de
un país extranjero que ha sustraído información crítica de varios de sus
clientes.

La empresa afectada, aconsejada por sus consejeros y abogados, ¿querría
llevar a juicio o iniciar algún tipo de acción legal?

Probablemente no.
```

El caso hipotético planteado se resuelve consiguiendo responder a todas las cuestiones que permiten tomar una decisión con conocimiento de causa. Sin embargo, esto no es siempre así y mucho menos cuando se está iniciando una investigación. Es importante gestionar las expectativas de la empresa respecto a las posibilidades de resolución, por lo que en todo momento se debe hablar de posibilidades. El desarrollo de una investigación digital correcta en sus procedimientos y conclusiones, no asegura el éxito del mismo. La experiencia del experto en seguridad hace que la balanza se incline hacia uno u otro lado, sin embargo, hay muchos aspectos que pueden dificultar o impedir el éxito de la labor del mismo, como las acciones que haya podido tomar, con la mejor de las intenciones, el equipo de sistemas a la hora de tratar de solucionar lo que a ellos se les presentaba como un problema y no como un incidente de seguridad.
Si es claro que independientemente de cómo se desarrolle el caso, éste no acabará en un juicio, el nivel de exigencias y pulcritud se relaja dejando paso a la efectividad en la investigación.
Además, no hay que olvidar que el proceso de la recogida de evidencias y de todo el análisis atendiendo de forma rigurosa a los procedimientos adecuados demanda una mayor dedicación y en el mundo profesional el tiempo es dinero. En cada escenario es necesario valorar si la inversión económica, el porcentaje de posibilidades de éxito y el propio desgaste del proceso hacen recomendable el inicio del mismo. Sin embargo, en aquellas actuaciones cuyo objetivo no es atender a un proceso judicial, sino obtener una determinada información, permiten una mayor flexibilidad, reduciendo con ello los tiempos dedicados a la recogida y tratamiento de evidencias.
La tendencia habitual es hacer uso de procedimientos que resultan algo imprecisos o inapropiados para tener valor judicial, pero que hacen énfasis en la efectividad y eficiencia de los resultados del análisis.

El proceso de investigación

El proceso de investigación (al que se como se conoce comúnmente como análisis confundiendo el todo con las partes, tal y como se ha comentado), se compone de cinco fases. Desde el inicio de la investigación, las fases se suceden de forma sucesiva y con dependencia de precedencia entre las mismas, de tal modo, que hasta que una fase no esta ejecutada y finalizada no se inicia la siguiente.
Este ciclo metódico a grandes rasgos y generalizando está compuesto por cinco fases: identificación, recopilación (recolección o adquisición), preservación, análisis y presentación.
Los procedimientos y técnicas seguidos por un investigador deben de estar basados en protocolos de actuación y en buenas prácticas. El proceso seguido por un investigador de seguridad debe situase dentro de unas determinadas características o condiciones:

- Marco científico: Tiene que estar basado en la ciencia y en la técnica.
- Marco metodológico: Tiene que seguir una metodología estructurada adecuada a la actuación.
- Proceso sistemático: Sus etapas o fases han de permitir que el proceso sea completo y exhaustivo.
- Proceso reproducible: Tiene que ser capaz de ser reproducible por un experto en la materia.

- Proceso auditable: Tiene que proporcionar las trazas necesarias para demostrar las tareas realizadas y los resultados obtenidos.

- Proceso comprensible: Tiene que ser comprensible por un experto en la materia.

Sin embargo, la propia idiosincrasia del entorno empresarial permite, y obliga en cierto modo, al investigador a presentar los resultados aplicando criterios de rentabilidad en tiempo y forma.
Es el investigador, profesional de la seguridad quien, en función de su experiencia y criterio, y conocedor de las expectativas y necesidades del cliente, determina en qué medida se alinea con las mejores prácticas exigidas para maximizar la diligencia con la que lleva a cabo su labor frente a la eficacia de los resultados que le son solicitados en tiempo.
A continuación se describen las fases de una investigación de seguridad básica, para la resolución de un caso, en el que no se contempla ningún tipo de proceso judicial. Esto es, el objetivo de la descripción de las fases será la optimización de la capacidad para conseguir un resultado determinado, en particular, presentar los resultados de la investigación a la empresa con el mínimo impacto económico. En capítulos posteriores ampliaré los aspectos adicionales de estas mismas fases, necesarios para desarrollar una investigación o peritaje forense.

Fase de identificación

La calidad de la información, así como acotar el ámbito de la misma es un factor crítico para el éxito de una investigación. Para un investigador es igualmente nocivo tanto el desconocimiento de información como el disponer de un volumen inmanejable de la misma. En el primer caso, el investigador puede llegar a conclusiones erróneas y en ambos casos puede no llegarse a presentar ningún resultado concluyente. Por lo tanto, es importante conocer los antecedentes concretos del caso, así como la situación actual. Esta información permitirá al investigador posicionarse y tomar las decisiones que le permitan determinar la estrategia a poner en práctica en la búsqueda de las evidencias.
Durante la identificación se debe:

- `Revisar el contexto legal` (ya que el hecho de que no se considere un proceso penal, no implica que se deba obviar que durante el proceso de investigación se pueda vulnerar la legislación vigente) que afecta al escenario, dispositivo, elemento o información que se va a analizar. Solicitar las autorizaciones necesarias, así como información referente a cuáles son los prerrequisitos, sobre qué se debe actuar, quién debe intervenir, quién puede estar presente y cuál es el limite de la actuación.

- `Planificar la investigación` e identificar las herramientas y los medios (hardware y software) así como los procedimientos, y los conocimientos necesarios para realizar una actuación profesional.

- `Identificar si la información existe en los dispositivos o debe ser capturada` en el proceso de la investigación (por ejemplo el trafico en la red 'online' origen y destino de las comunicaciones).

- `Identificar unitariamente los medios y bienes involucrados` susceptibles de contener cualquier tipo de información o evidencia relevante. No solo los dispositivos telemáticos sino también aquella documentación que pudiera contener información susceptible o afín.

- La `descripción de los dispositivos`: qué son cada uno de ellos, qué identificaciones existen en el dispositivo y cuáles proceden del fabricante o distribuidor, tipo de dispositivo, los posibles usos y utilidades de cada dispositivo para qué, quién, cuándo, dónde, con qué frecuencia, etc.

Fase de recopilación

Una vez identificados los diferentes dispositivos, la fase de recolección o adquisición, comúnmente llamada recopilación, implica la obtención y documentación del tipo de información y entorno del cual se deba extraer la información que forma la evidencia.
En muchos casos existe una sola oportunidad de capturar la información, por lo que esta operación se tiene que realizar en la secuencia adecuada y con las mayores garantías de que se va a obtener el resultado esperado.
La recopilación de información debe cumplir con dos requisitos:

- Respetar el orden de prioridad según la volatilidad de la información.
- Ser sistemático.

En línea con el cumplimiento de los citados requisitos se considera adecuado:

- Seguir directrices de buenas practicas reconocidas.
- Desarrollar listas de chequeo que permitan no pasar por alto ninguno de los pasos esenciales o elementos susceptibles de contener información relevante.
- Mantener un registro ordenado cronológicamente de la actuación de recopilación de la información. Las diferentes entradas se deben de complementar con cualquier dato que se encuentre, sean o no significativos, y cualquier incidencia que surja durante el proceso.

Durante la recopilación se tiene que ser extremadamente cuidadoso y asegurar que siempre se está trabajando dentro de las condiciones y requisitos de legalidad que requieren estas situaciones. De nuevo, aunque no se tenga en mente tomar acciones penales, es necesario tomar las medidas necesarias para no violar el contexto de privacidad que se debe preservar y contar con las autorizaciones adecuadas del propietario de los equipos o responsable de los sistemas o de la empresa.

Fase de preservación

La correcta ejecución de esta fase es clave para la ejecución de una investigación profesional. Quizás sea por eso que, de todas las fases, sus tareas son las más conocidas incluso por gente con poco conocimiento en el área de la investigación de seguridad, pero sobretodo, como se explicará posteriormente, por las personas que se inician en el ámbito pericial o forense.
Las tareas de preservación tienen como objetivo el disponer de una copia idéntica e integra (también llamada imagen de disco) de los datos contenidos en los dispositivos a analizar.
La fase de recopilación lleva implícitas acciones que implican la manipulación de las evidencias recopiladas ya que la identificación de las mismas implica el uso de herramientas de búsqueda, localización, composición y procesos que podrían de un modo u otro alterar o contaminar el contenido de las mismas.
Es por ello que, previo al inicio de las tareas de recopilación, el investigador debe de realizar dos copias (como mínimo) de los datos contenidos en los dispositivos, con los que posteriormente se va a trabajar.
La copia original se guarda en custodia, la primera copia se utiliza para continuar con las fases de la investigación y, en caso de tener que reproducir una prueba, dado que la primera copia ya ha sido alterada, se volvería a obtener una nueva copia de la segunda copia realizada.
No es menos cierto que, si bien en este punto el ámbito de actuación no contempla acciones judiciales, donde este tipo de protocolo es un requisito imprescindible como se verá en los siguientes capítulos, una mala o descuidada praxis de las tareas de preservación no es considerada una práctica profesional.
Uno de los requisitos de una investigación correcta es que debe de ser repetible, y si no se dispone de la posibilidad de reproducir la situación de partida de forma íntegra, es imposible cumplir con el requisito.

Es muy importante utilizar las medidas necesarias en cada caso para evitar la modificación, borrado o sobregrabado accidental durante el proceso de copia.
Las copias realizadas se tienen que identificar unívocamente, de forma que se pueda verificar su exactitud y no manipulación. Es habitual, para este tipo de tareas, el uso de programas que utilizan las funciones 'Hash' (o Checksum) para verificar la integridad de las copias de los datos.
Ante la inminente realización de la replica de los datos el investigador tiene que considerar diferentes aspectos importantes del contexto para determinar el proceso a seguir como:

- Si el dispositivo esta arrancado:
  - ¿Es conveniente de apagarlo o mantenerlo encendido?
- Si el dispositivo no esta aislado de las comunicaciones (físicas o inalámbricas).
  - ¿Cómo actuar para preservar su aislamiento de actuaciones de terceros sin alterar la información contenida?
- Si el dispositivo es modular:
  - ¿Qué elementos o partes de los dispositivos identificados que pueden contener información (como memoria RAM, discos ópticos, tarjetas de memorias) son prioritarios?
- ¿Qué herramientas hardware y/o software son necesarias para la realización de la replica con garantías e integridad para cada dispositivo o elemento.
- ¿Qué particularidades tiene cada dispositivo?
- ¿Qué proceso o protocolo es necesario seguir en cada caso?
- ¿Qué elementos de intercomunicación o interfaz se necesita para interactuar con el dispositivo y realizar la copia?
- ¿Qué elementos o soportes son necesarios para mantener o conservar la copia de las evidencias de los dispositivos (medios de soporte de la copia, capacidades, numero de soportes, etc.)?

Las respuestas a estas cuestiones vienen determinadas por las buenas prácticas, las metodologías utilizadas y la experiencia del investigador.

Fase de análisis

Tal y como se indica anteriormente, las tareas propiamente dichas de análisis de los datos se aplican sobre los medios duplicados, nunca sobre originales.
Un investigador o analista profesional[4]:

- Es `metódico y sistemático`. Basa su labor en el método científico, es decir, planteando hipótesis y encontrando evidencias que la refrenden.
- Trabaja de forma `repetible`. Tiene que permitir replicar los pasos del análisis de los datos que nos permiten llegar a la obtención de las conclusiones sobre lo que se desea conocer o determinar, y obtener los mismos resultados.

[4]Yo defiendo que si el profesional sólo participa en la fase de análisis es *analista* y en cualquier otro caso se trataría de un *investigador*. Esto se debe a que, hasta donde llega mi conocimiento, no existe un perfil de 'identificador', 'recopilador', 'preservador' o 'presentador' profesional, asociado a casa una de las fases.

- Toma decisiones `razonadas`. El conjunto de decisiones y acciones posteriores que conforman un análisis están basadas, en la medida de lo posible, en buenas practicas, de modo tal que el mismo pueda ser refrendado y mostrado ante terceros especialistas garantizando el correcto proceder del proceso de análisis llevado a cabo.

Cada análisis es particular y propio en función de los antecedentes conocidos, el objetivo perseguido, los medios en cuestión y las evidencias que se hayan podido recolectar y el estado de las mismas.
Existen procedimientos genéricos para soportar las técnicas de análisis y búsquedas de evidencias particulares y especificas de la investigación que se este llevando a cabo. Estos procedimientos técnicos facilitan las pautas para realizar el análisis, por ejemplo, de:

- Los diferentes sistemas operativos de los fabricantes como Microsoft, Apple, distintas distribuciones de *nux.
- Los diferentes tipos de redes (ethernet, inalámbricas) y protocolos soportados por las mismas (IEEE 802).
- Dispositivos de información diferenciados (discos, memorias del PC, memorias portátiles, teléfonos y dispositivos inteligentes).
- Tipología de la información (ficheros gráficos, ofimáticas, texto plano como logs, pdf).

Mediante el uso de técnicas de análisis basadas en procedimientos y herramientas técnicas se llega a extraer los datos que conforman la información que, a su vez, tras ser analizada y contextualizada, da respuesta a las cuestiones que plantean las investigaciones. Sin embargo, esto no siempre es una tarea sencilla y la información puede estar contenida en distintos datos dispersos, o que parte de los datos que conforman dicha información hayan sido eliminados o el disco puede haber sido formateado o dañado, y esto hace que sea necesaria la aplicación de técnicas y herramientas especificas para recuperar la información.
En función del estado de la información, es recomendable contar con los servicios especializados de expertos en este tipo de actividades que contribuyan a la obtención de la información y a la preservación de la misma.
Otra de las tareas del análisis es la obtención de la información no visible de los ficheros, como los metadatos, cuya utilidad ha sido probada empíricamente en varios casos ya que ha permitido conocer cual ha sido el ciclo de vida del mismo, fechas/horas, autoría de la creación, accesos, modificaciones, entre otros datos.
Finalmente, el analista debe de desarrollar, como parte del análisis un:

- Mapa de actores e interacción: Son actores a considerar los usuarios, máquinas, los programas, los accesos y los destinos de las comunicaciones, las interacciones, con quien, donde, cuando, con que frecuencia, que información es de cada usuario, sus accesos a la maquina, permisos de trabajo y privilegios, etc. A través de la información de los accesos y de los registros es posible conocer quienes son los actores principales del escenario.
- Cronología o reconstrucción relacional: Linea temporal o cronología de los acontecimientos, de su interpelación y vínculos a lo largo del tiempo. Esta información se complementa con las evidencias de cómo se relaciona el conjunto y los elementos mas significativos de la cronología.

Una buena cronología acompañada de un mapa o esquema relacional permite entender mejor la situación, como ha transcurrido la misma y con ella determinar cuales son los momentos importantes y las evidencias que pueden refrendar o aportar información sobre lo acontecido.

Fase de presentación

El análisis de la información y las evidencias, permiten al investigador llegar a una conclusión determinada. Esta conclusión debe quedar reflejada en un informe con un enfoque claro, preciso y entendible por terceros que no estén vinculados con el tema, con independencia de que el informe tenga carácter judicial o extrajudicial.

Si bien normalmente no es requerido por las empresas, en esta fase se recomienda guiarse por documentos de referencia o protocolos como pudieran ser la norma UNE 197001:2011.

Es importante recalcar que el informe debe ser comprensible para personas no expertas en la materia y, al mismo tiempo, también tiene que auto contener la información técnica suficiente y necesaria (aunque sea en apartados anexos) para poder ser entendida y comprendida por técnicos especialistas o expertos en la materia tal y como lo es el propio investigador que elabora el informe.

Durante la reunión de entrega del informe al peticionario o gestor del encargo se da una explicación sobre el contenido del informe y se aclaran las dudas pertinentes, en caso de que surjan. Esto facilitará en gran medida la comprensión del contenido del mismo por los interesados.

Un informe tiene que ser profesional, riguroso, respetuoso, previsor y argumentativo. Es responsabilidad del investigador conservar copia de todo lo necesario, utilizando los medios que garanticen la integridad y confidencialidad de las misma para poder, en un momento dado, rememorar todo el proceso y las actuaciones, siendo capaz de realizar una exposición o dar las pertinentes explicaciones que le sean solicitadas.

Capítulo 3: INVESTIGACIÓN INFORMÁTICA FORENSE

Investigación informática forense

En algunos libros se habla de Informática Forense[1], definiéndose el concepto como 'conjunto multidisciplinario de teorías, técnicas y métodos de análisis que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática'. Y sintetizan en una frase su significado:
La Informática Forense es a la Informática lo que la Medicina Legal es a la Medicina.
Expongamos a continuación, de nuevo, un caso hipotético y que recoge situaciones que no son inusuales en la realidad y que ilustran la posibilidad de que una investigación desemboque en un proceso judicial.

Se detecta un aumento de tráfico inusual asociado a un servidor de la DMZ de la empresa y, los primeros datos de la investigación, identifican que el origen del mismo es un servicio P2P no identificado en la CMDB de los sistemas de dicha empresa.

En consecuencia se decide continuar con la investigación y averiguar que está ocurriendo. Se detecta la presencia de un cliente P2P instalado en el servidor.

En ese momento son múltiples las cuestiones a abordar: ¿por qué el antivirus no lo ha detectado?, ¿pueden otros servidores estar afectados?, ¿quién lo instaló?, ¿cuándo se instaló?, ¿qué tipo de información ha transmitido?, ¿es recomendable eliminarlo?

Sin embargo, en el transcurso de la investigación digital no sólo se detecta al elemento malicioso, sino que se evidencia una fuga de información crítica para el negocio.

Se localiza quién ha sido el culpable de la acción maliciosa y a qué tipo de información ha tenido acceso que evidencia un alto riesgo de impacto negativo en la imagen de la empresa. La información analizada indica que se podría tratar de un grupo de lammers o script-kiddies de un país extranjero que ha sustraído información crítica de varios de sus clientes.

La empresa afectada, aconsejada por sus consejeros y abogados, ¿querría llevar a juicio o iniciar algún tipo de acción legal?

Supongamos que la respuesta es =sí=.

Tanto si la respuesta es una afirmación clara y rotunda, como si cabe la más mínima duda de que la investigación tenga implicaciones judiciales se requiere plantear el desarrollo del mismo dentro del ámbito judicial, o en otra palabra, ámbito forense.
Adicionalmente, la respuesta afirmativa a dicha cuestión, quién debe enfrentar dicha situación, cómo enfrentarla, y el editor de textos Emacs como herramienta básica para la investigación forense resume el objetivo planteado en este PFC.
Es importante, y se repetirá a lo largo del PFC, que en una investigación informática forense:

- El investigador gestione las expectativas del cliente en relación a las posibilidades reales de resolución del proceso judicial. En este sentido es igualmente importante, y de nuevo se plantea la

[1] MANUAL DE INFORMÁTICA FORENSE I. Darahuge, María Elena/Arellano González, Luis E. ISBN-10: 9870112498 Aparición: 10/08/2011 Páginas: 416

relevancia del adecuado uso del léxico, en todo momento hablar de `posibilidades`. El desarrollo de una investigación forense correcta en sus procedimientos y conclusiones, no asegura el éxito de la misma desde el punto de vista del cliente, ya sea porque los resultados de la investigación no se alineen con sus expectativas, por falta de evidencias o por la propia decisión del juez.

- Las acciones desarrolladas desde el primer momento deben atenerse a un alto grado de pulcritud y rigor procedimental dado que las conclusiones obtenidas a partir de las evidencias identificadas, preservadas y analizadas deben de ser válidas, creíbles, rotundas e irrefutables con el fin de que el juez disponga de toda la información necesaria como para tomar una decisión correcta.

Sin embargo, si bien para acometer una investigación forense el investigador hace uso de metodologías y procedimientos que, siendo más o menos reglados, pueden resultar algo imprecisos o incluso inapropiados para el proceso judicial.
Por ejemplo, en relación con la última afirmación, un investigador forense puede hacer uso de las normas especificadas en la RFC 3227 'Guía para la recogida y almacenamiento de evidencias' (Guidelines for Evidence Collection and Archiving), para tareas de adquisición de evidencias. En países avanzados judicialmente en materia de procedimientos forenses informáticos, que incluso disponen de leyes y regulaciones para ello, esta RFC pueda tener su validez. Sin embargo, en España, aplicar esta norma de forma escrupulosa puede no ser prudente ya que no sigue escrupulosamente el principio de 'antes de tocar cualquier evidencia, prevalece la rigurosa recogida de la misma'. La imparcialidad del investigador forense es obligatoria por ley, sin embargo, dado que sus servicios son contratados normalmente por una de las partes, la independencia asociada a su labor puede ser cuestionable.
Por lo tanto, para el investigador forense es decisivo disponer de los medios para poder probar y afirmar, en cualquier caso, que cuando llegó, el escenario 'ya estaba así'. En caso contrario, las evidencias pueden ser recusadas por posible alteración de las mismas durante la fase de análisis, ya que el escenario nunca debe ser alterado.
Todos estos aspectos clave se desarrollarán a lo largo del PFC.
Adicionalmente, se tratará de concienciar acerca de la relevancia del proceso que se tiene entre manos, de la necesidad de anticiparse a las cuestiones a abordar antes de hacerlo y la importancia de conocer las metodologías y herramientas necesarias para ello.

El perito informático

Tal como se explicó en el apartado '¿Por qué lo llaman análisis cuando quieren decir investigación?' del anterior capítulo, un peritaje o peritación es el estudio o trabajo que hace un perito y la definición de este tipo de profesionales es aquella persona entendida, que posee conocimientos y experiencia dentro de la informática y las tecnologías, en cualquiera de sus diferentes ramas y especializaciones en las que se le reconoce como experto y que es capaz de asesorar, dar opinión o elevar un dictamen para otras personas, de forma comprensible para las no entendidas en la materia y, al mismo tiempo, especializada para los expertos como él, en los campos o especializaciones que se estén tratando.
En el apartado anterior se ha establecido la relación entre la investigación forense y los procesos judiciales. Sin embargo, el aparato judicial no reconoce la figura de `investigador de oficio` o `analista de oficio`, sino que manejan la figura del `perito de oficio`. Dentro de dicho contexto, un perito informático forense es un auxiliar del aparato judicial, representado por el tribunal interventor. En ningún caso va a decidir sobre el resultado de un caso, ya que esa es responsabilidad exclusivamente del órgano juzgador.
Un perito forense utilizará métodos de investigación forense para el ejercicio de su profesión. Fuera de España es normal utilizar términos como Digital forensics investigations, *first responder*, electronic discovery, digital forensic technician, digital evidence examiners, y otros tantos para referirse a los actores y actividades relativas a la investigación forense.

A lo largo del presente PFC se utilizará indistintamente el concepto de `investigador forense` y `perito forense`, siempre dentro de un entorno informático o digital.
En los siguientes apartados se pretende poner en contexto la figura del profesional, auxiliar del aparato judicial español. Es por ello que, en este caso, me refiero a el mismo directamente como *perito forense*.

Perito forense: Objetivo

Según la wikipedia, en relación con el delito informático en España:

```
En España, los delitos informáticos son un hecho sancionable por el
Código Penal en el que el delincuente utiliza, para su comisión,
cualquier medio informático. Estas sanciones se recogen en la Ley
Orgánica 10/1995, de 23 de Noviembre en el BOE número 281, de 24 de
noviembre de 1995. Éstos tienen la misma sanción que sus homólogos no
informáticos. Por ejemplo, se aplica la misma sanción para una
intromisión en el correo electrónico que para una intromisión en el
correo postal.

El Tribunal Supremo emitió una sentencia el 12 de junio de 2007 (recurso
N° 2249/2006; resolución N° 533/2007) que confirmó las penas de prisión
para un caso de estafa electrónica (phishing).

A la hora de proceder a su investigación, debido a que una misma acción
puede tener consecuencias en diferentes fueros, comenzará la
investigación aquel partido judicial que primero tenga conocimiento de
los hechos delictivos cometidos a través de un medio informático, si
durante el transcurso de la investigación, se encuentra al autor del
delito y pertenece a otro partido judicial, se podrá realizar una acción
de inhibición a favor de este último para que continúe con la
investigación del delito.
```

Según la legislación española, un delito informático podría definirse como aquel hecho tipificado como delictivo en el código penal, pero que para ser cometido, se hayan utilizado técnicas o mecanismos informáticos. Ejemplos de delitos informáticos podrían ser la estafa, extorsión, ataques a la propiedad intelectual o casos de pornografía infantil, terrorismo o crimen organizado.
El objetivo final del peritaje informático es la reconstrucción del hecho a partir de la prueba indiciaria, que se identifica, recolecta, certifica y resguarda en la escena del delito.
En ese sentido, desde el punto de vista criminalístico, los objetivos son:

- Investigar técnicamente y demostrar científicamente la existencia de un hecho en particular, que probablemente sea delictivo.
- Reconstruir los hechos acaecidos, determinando los fenómenos ocurridos y los mecanismos utilizados, señalando los instrumentos u objetos de ejecución, sus manifestaciones y acciones que se pusieron en juego para realizarlo.
- Aportar evidencias siguiendo el proceso de obtención y custodia adecuados, para la identificación del o los presuntos autores.

En resumen, se puede afirmar que, en la mayoría de los casos, el peritaje forense informático está enfocado hacia el tratamiento y la confección de los medios de prueba por medio de las evidencias informáticas.

Esta rama del peritaje, como veremos más adelante, es la más técnica y cercana a la tecnología en sí misma. Sin embargo, como se desarrollará más adelante, de forma generalizada los servicios de un perito informático tienen uno de los siguientes objetivos:

- El desarrollo de un informe pericial (dictamen pericial, estudio, tasación o auditoría), ya sea en el ámbito extrajudicial o judicial (forense, de lesión, tasación o auditoría).
- El desarrollo de una actividad de asesoramiento, en actividades de consultoría, mediación y arbitraje.

Como ya se ha comentado, el hecho de que se trate de un área de especialización multidisciplinar, en su sentido intrínseco, implica que abarca multitud de áreas y especialidades en función de los dispositivos, lenguajes, redes, infraestructuras, entre otras, sobre la cual se esté tratando y exigen estar al día de las nuevas tecnologías.
En los casos en los que se ven involucradas tecnologías muy concretas y dispares es necesario recurrir a un equipo de peritos para abarcar todas las áreas de especialización requeridas.

Perito forense: Perfil

Un perito informático es un *profesional experto en la materia* en la que es requerido. La cualificación debe de estar avalada por las titulaciones y las experiencias propias de cada perito, adquiridas a lo largo de su trayectoria profesional.
El perito debe de actuar siempre según sus capacidades profesionales, por lo que debe de ser extremadamente consciente de sus limitaciones técnicas, y aislar sus opiniones personales y prejuicios del trabajo realizado.
Sin embargo, no basta con disponer de conocimientos técnicos. Es igualmente necesario 'conocer la profesión', esto es, disponer de conocimientos específicos sobre legislación, metodologías, buenas practicas, procedimientos y entandares, entre otros, que resultan imprescindibles para proporcionar las características y garantías exigibles a la labor del perito, para obtener un resultado objetivo, metódico, sistemático reproducible, demostrable, auditable, neutral, veraz, creíble, honesto y profesional.
Como parte del conocimiento de la profesión, el perito debe de conocer las siguientes leyes:

- Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil (LEC).
- Ley de Enjuiciamiento Civil (anterior) 1881 (LECa).
- Ley de Enjuiciamiento Criminal 1881 (LECrim)
- Ley Orgánica 6/1985 de 1 de julio, del Poder Judicial (LOPJ).
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (CP)
- Constitución Española 1978 (CE).
- Código Civil español (CC) RD 24 de julio de 1889.

Como profesional, al perito se le exige:

Objetividad ser una persona completamente ajeno al proceso en el cual se le requiere o se presenta su participación.

Imparcialidad ser una persona totalmente ajeno a los intereses particulares objeto del caso.

Conocimiento ser una persona que posea una formación como experto, ya sea reglada o fruto de la experiencia de sus desempeños, conocimientos especializados, científicos, artísticos o prácticos según a el caso o la temática para la cual es requerido su dictamen especializado.

Voluntariedad ser una persona que sin ningún tipo de coacción acepte aplicar sus conocimientos al proceso.

En cualquier caso, el perito, como experto y persona con una relación laboral con el caso, será adecuadamente remunerado con sus honorarios independientemente del resultado de su investigación.

Perito forense: Requisitos

En la definición de perito no aparece referencia alguna al tipo de titulación o nivel de estudios requeridos. Esto se debe a que no es necesario disponer de titulaciones concretas para ser reconocido como perito.
Esto es un grave problema que no parece que tenga solución a corto plazo. Comparando la situación de la informática forense con la medicina legal se aprecia un abismo en los temas relativos a requisitos necesarios para su profesionalización. La medicina legal es una especialización dentro de la medicina, sin embargo no existe dicho concepto dentro de la informática. Como única excusa plausible, podríamos aceptar que la medicina ha dispuesto de siglos de evolución frente a los pocos años de vida que tiene la informática.
Sin embargo, durante la preparación de este PFC, he identificado una serie de iniciativas, muchas de ellas privadas, que tienen como objetivo poner cierto orden en un negocio donde todo el mundo intenta abarcar lo máximo posible para competir dentro de un mercado muy saturado.
Actualmente sólo existen dos especialidades en el ámbito pericial, Medicina y Derecho, en las cuales los profesionales tienen la obligación de estar colegiados.
Desde estas líneas me gustaría abogar por la necesidad de que los responsables de definir los planes de estudios futuros dentro de la informática, se planteen la posibilidad de aprender del mundo de la educación en materia de medicina y plantear un escenario educativo similar.
Fuera del mundo educativo existen, según la Ley de Enjuiciamiento Criminal (LECrim) en su artículo 457, dos tipos de peritos:

Peritos titulares Profesionales que tienen título oficial de ciencia o arte cuyo ejercicio esté reglamentado por la Administración. El título oficial puede estar expedido por una Universidad, Asociación o Colegio Profesional, o un centro reglado de formación.

Peritos no titulares Profesionales que, careciendo de título oficial poseen, disponen de conocimientos o prácticas especiales en alguna ciencia o arte. Estos conocimientos son los que lo hacen experto y reconocido en la materia, dentro del entorno y del contexto de profesionales que se dedican a dicha ciencia o arte.

Por otro lado, según el artículo 340.1 de la Ley de Enjuiciamiento Civil (LEC), los peritos deberán poseer el titulo oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. Si se tratase de materias que no están comprendidas en títulos profesionales oficiales, el perito será nombrado entre personas entendidas en esta materia aunque no queda explicitado cómo podrá acreditarse la condición de persona entendida. Esto implica que un experto sin titulación puede actuar como perito, con idénticos derechos y deberes, pero estas personas han de acreditar los conocimientos especializados como los de una persona que, careciendo de título oficial, es experta en la materia en cuestión sobre la que se acredita no estando la misma comprendida en títulos profesionales oficiales.
Adicionalmente, la LECrim, en su artículo 458 establece que el Juez, existiendo peritos titulares, se valdrá con preferencia de estos para los procesos judiciales. Adicionalmente, en los procesos judiciales

actuando de oficio, habiendo peritos en posesión de titulación oficial, tendrán preferencia en la asignación por parte del Tribunal.
Por lo tanto, para los profesionales que quieren orientar su actividad a trabajar como perito de oficio en los temas judiciales y oficiales, deberán poseer el título oficial que corresponda a la materia objeto del dictamen y a la naturaleza de éste. En el caso de peritos que actúen de forma extrajudicial o judicialmente de parte, no es necesario tener titulación alguna (si bien, en cualquier caso, es recomendable) considerando que su elección y contratación queda a criterio de la parte o cliente bajo su cuenta y riesgo.

Perito forense: Marco

Un caso, proyecto, investigación o actividad que lleve a cabo un perito informático está enmarcado como judicial o extrajudicial.

Marco Judicial Actividades reguladas por la Ley de Enjuiciamiento Civil (LEG), dentro de un procedimiento judicial, y por la Ley de Enjuiciamiento Criminal (LECrim), como caso penal.

Marco extrajudicial Actividades que se realizan dentro del ámbito particular. El dictamen, dada la metodología y medios utilizados, puede ser utilizado como paso previo para una demanda judicial. Sin embargo, dicho dictamen puede ser utilizado para la toma de decisión, tasación, mediación o valoración de los bienes informáticos, tal y como se verá.

- Marco judicial

  El perito judicial:

  - Debe de aportar elementos de prueba.
  - Debe de ser honesto e imparcial.
  - Debe asesorar al tribunal en cuantas cuestiones se planteen y requieran acerca de su ámbito de especialización.

  El perito judicial puede ser designado:

  Por designación de las partes cualquiera de las partes que intervienen en un proceso judicial pueden designar su propio perito, aportar sus dictámenes y pericias tanto en la formulación de la demanda o la contestación a la misma. En este caso no es necesario que el profesional esté dado de alta en las listas del juzgado ni que pertenezca a ninguna lista de un Colegio o Asociación que estén dados de alta en el juzgado, si bien deberá de poder avalar su cualificación como perito.

  Por designación del Tribunal Para poder ser nombrado como perito designado por el Tribunal, el profesional debe estar dado de alta en las listas que obran en los Juzgados en las cuales no se puede incorporar un profesional individualmente sino que debe ser por medio de los Colegios Asociaciones Profesionales. Esta designación puede ser requerida:

  Sin instancia de las Partes La ley establece que el Tribunal podrá, de oficio, designar perito cuando la pericia sea pertinente y así lo considere por ser necesarios conocimientos específicos para dirimir las cuestiones que se le plantean.

  A instancia de las Partes La Ley establece que si una de las partes es titular de derecho de asistencia gratuita, con simplemente anunciarlo, se procederá a la asignación de un perito judicial.

- Marco extrajudicial

  El peritaje extrajudicial surge de las relaciones entre los particulares, profesionales y las empresas cuando surgen situaciones en las que es necesario un experto para que pueda asesorar o informar sobre la materia en cuestión, aportando una visión objetiva, imparcial y experta para la posterior toma de decisiones.

  Las actuaciones extrajudiciales suelen ser más extensas debido a que en estas situaciones se trata de analizar una problemática desde su globalidad, identificando los posibles puntos de interés y circunstancias que pudiesen ser tenidos en cuenta en un hipotético juicio.

  El informe pericial sirve para resolver el conflicto y llevar a cabo la negociación de modo tal que no sea necesario llegar a los Tribunales. En caso de que se decida acudir al marco judicial, el informe pericial es el elemento de prueba presentable junto con la demanda, tanto para el demandante como para el demandado, si es un peritaje de defensa o de respuesta a la demanda.

Perito forense: Ámbito

Si bien puede parecer que el hecho de que el PFC se centre en los procesos judiciales implica que es de aplicación únicamente en el ámbito penal, esto sería una gran imprecisión. Un proceso judicial no se limita al ámbito penal.
El ámbito de actuación, dentro de un proceso judicial, de los peritos informáticos es muy amplio, ya que debe dar cobertura a diferentes problemáticas que se puedan dar en el basto mundo de los conflictos informáticos.
A continuación se enumeran ejemplos de algunos de los ámbitos en los que puede verse involucrado un perito informático:

- Ámbito penal

  Como ya se ha comentado anteriormente, según la legislación española, un delito informático podría definirse como aquel hecho tipificado como delictivo en el código penal, pero que para ser cometido se hayan utilizado técnicas o mecanismos informáticos.

  Ejemplos de situaciones, dentro del ámbito penal, en los que es requerido un perito informático, son:

  - Delitos de carácter económico, societarios o contra el mercado o derechos de los consumidores.
  - Revelación de secretos.
  - Espionaje intelectual o industrial.
  - Delitos relacionados con el uso ilegal de software.
  - Vulneración de sistemas de la empresa.
  - Vulneración de la intimidad de los trabajadores a través de correos electrónicos, comunicaciones u otros medios.
  - Delitos contra la confidencialidad, integridad o disponibilidad de sistemas de información electrónicos en empresas o a particulares.
  - Delitos contra la confidencialidad, integridad o disponibilidad de comunicaciones electrónicos en empresas o a particulares.
  - Delitos relacionados con la venta electrónica fraudulenta.
  - Delitos por acoso a personas.
  - Delitos contra menores y pornografía informática.

- Delitos contra el honor y la intimidad de las personas.

- Ámbito laboral

  Las relaciones laborales que se establecen entre la empresa y sus colaboradores y trabajadores en sus múltiples formas, establece obligaciones basadas en la buena fe y respeto mutuo de los derechos, así como una relación de confianza y de profesionalidad.

  El incumplimiento de las obligaciones contractuales o de los convenios colectivos, estando estos vinculados a sistemas informáticos, es otro de los ámbitos de actuación de un perito informático.

  Ejemplos de situaciones del ámbito laboral que pueden derivar a acciones dentro del ámbito penal, en los que es requerido un perito informático, son:

  - Revelación de información confidencial.
  - No preservación del secreto profesional.
  - Incumplimientos de las normativas de seguridad o de la protección de datos.
  - Uso indebido (ilegal o abusivo) de los recursos de la empresa.
  - Abuso de poder de la empresa sobre sus colaboradores en sus funciones de control y gestión de servicios como el correo y comunicaciones
  - Invasión de la intimidad del colaborador o trabajador por medio de los equipos informáticos.

- Ámbito administrativo

  El ámbito administrativo abarca los casos relativos a procesos en los que una de las partes es la Administración Pública.

  Ejemplos de situaciones del ámbito administrativo que pueden derivar a acciones dentro del ámbito penal, en los que es requerido un perito informático, son:

  - Problemas derivados del uso de los medios electrónicos puestos por la Administración al alcance de los ciudadanos y de las empresas.
  - Manipulación o mal uso del DNI electrónico.

- Ámbito mercantil y civil

  Un perito informático puede ser contratado para mediar en temas concernientes al cumplimiento de las obligaciones contractuales que se establecen en el ámbito de las relaciones mercantiles, comerciales o entre los particulares.

  Normalmente se producen situaciones en las que el demandante queda legitimado para reclamar al demandado una cantidad económica en concepto de daños ocasionados por el incumplimiento de este último o a restituir o reparar el daño causado.

  Ejemplos de situaciones del ámbito mercantil y civil que pueden derivar a acciones dentro del ámbito penal, en los que es requerido un perito informático, son:

  - Incumplimiento de obligaciones contractuales:
    - Trabajos inacabados o abandono.
    - Alcance de lo contratado.
    - Falta de capacidad técnica u operativa.

Perito forense: Actividad

Si bien el PFC se centra en un tipo de actividad específico de peritaje informático forense, a continuación se enumeran y definen brevemente éste y otros tipos de peritos informáticos con el fin de poder diferenciarlos y no confundir su actividad.

Perito informático forense Peritaje que se realiza cuando se utilizan técnicas especializadas en el análisis de tecnologías, para identificar y localizar evidencias en los dispositivos, redes, memorias, discos, sistemas, productos, programas, entre otros.

Perito de gestión o de management Peritaje cuya actividad implica la utilización de técnicas especializadas en el análisis y la búsqueda de evidencias de los incumplimientos y deficiencias en contratos, proyectos, implementaciones, entregables, defectos ocultos, servicios, niveles comprometidos, estándares, normativas y buenas practicas, entre otros. Adicionalmente, dentro del apartado actual se identifican como:

Perito auditor Peritos cuya labor implica el uso de técnicas de análisis para establecer y dar fe sobre el cumplimiento con la legislación, las normas y los estándares, así como recomendaciones para la mejora o subsanación de las deficiencias a incumplimientos detectados durante el proceso de auditoría.

Perito mediador Peritos cuya labor implica el uso de técnicas de análisis de situaciones, de negociación de conflictos y de resolución de problemáticas entre las partes sujetas al proceso de mediación.

Perito tasador Peritos cuya labor implica el uso de técnicas para evaluar el valor de las cosas, en función del valor del mercado, valor de reposición, valor amortizado, tiempo de adquisición, funcionamiento, nivel de obsolescencia y coste de mantenimiento, entre otros.

Principios básicos a seguir

Ya se ha hablado de la objetividad y la rigurosidad que se le presupone al perito a la hora de desarrollar su labor.
Rene Descartes, filósofo, matemático y físico francés, considerado el padre de la filosofía moderna, así como uno de los nombres más destacados de la revolución científica, propone un método que ha de ser matemático y universal, sea cual sea su aplicación o campo del saber a que se refiera. La definición de lo que él entiende por método la podemos encontrar en la Regla IV de su obra 'Regulae ad directionem ingenii':
'Así pues, entiendo por método reglas ciertas y fáciles, mediante las cuales el que las observe exactamente no tomará nunca nada falso por verdadero, y, no empleando inútilmente ningún esfuerzo de la mente, sino aumentando siempre gradualmente su ciencia, llegará al conocimiento verdadero de todo aquello de que es capaz.'[2]
La primera ventaja que nos proporciona el método es evitar el error. Pero, además de proporcionarnos un conjunto de reglas o procedimientos para deducir lo que ya conocemos, puede aplicarse a cualquier nuevo campo del saber. El método permitirá que aumentemos nuestros conocimientos y descubramos nuevas verdades.
Con el Discurso del Método, de Rene Descartes, se establece una nueva forma de pensamiento en la que se cuestionan los dogmas de fe, se promueve la necesidad de tomar una actitud crítica y objetiva de investigación, libre de imposiciones, que es la base del pensamiento moderno.
Descartes propone cuatro reglas que fundamentan el método científico y que yo resumiría como:

[2] 'Reglas para la dirección del espíritu'. Alianza editorial, Madrid 1989, pg. 79

1. No admitir jamas nada como verdadero sin disponer de una evidencia que lo corrobore.

2. Dividir cada problema en tantos subproblemas como fuere posible y se requieran para obtener la mejor solución.

3. Ordenar los pensamientos, empezando por los objetos más simples y mas fáciles de conocer, para ascender gradualmente hasta el conocimiento de los más compuestos, e incluso suponer un orden entre los pensamientos que no se preceden naturalmente.

4. Hacer recuentos tan integrales y revisiones tan generales, que permitan asegurar que no se omite nada.

Existen una serie de principios básicos y teóricos que se han de tener en cuenta en la realización de cualquier tipo de análisis que conlleve la generación u obtención de unas conclusiones sobre el mismo. Estos principios no son dogmas de fe, sería una incongruencia después de plantear los fundamentos de método científico, pero hay determinadas prácticas que son aplicables el ámbito de este PFC, con independencia del tipo de labor que se esté realizando (peritaje, mediación, tasación o auditorías).
El sentido común, que en muchas ocasiones es el menos común de los sentidos, es un argumento básico en muchas investigaciones, y mencionar alguno de los siguientes principios en la redacción del informe o dictamen puede ser recomendable para apoyar el criterio o la decisión que se ha tomado a la hora de realizar determinadas actuaciones.
El principio de intercambio o de transferencia de Locard.
Planteado por Edmond Locard (1877-1966), criminalista francés pionero en su época, desarrolló una serie de principios metodológicos que, aplicados a determinadas pruebas, las convertían en evidencias irrefutables ante un juez.
El principio de Locard establece que 'Siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto'.
Esto implica que, en toda ocasión, cuando se entra en contacto con un objeto o sustancia se da un intercambio material. Se ha demostrado en muchas ocasiones que, analizando dichos rastros, se puede conocer mucha información acerca de personas implicadas, secuencia de sucesos y procesos desarrollados.
En el ámbito del peritaje informático, un ejemplo del principio de intercambio serían los metadatos que quedan en las imágenes al realizar una fotografía.
Principio de Indeterminación o de incertidumbre de Heisenberg.
Este principio revela una característica distinta de la mecánica cuántica que no existe en la mecánica newtoniana. Como una definición simple, podemos señalar que se trata de un concepto que describe que el acto mismo de observar cambia lo que se está observando. En 1927, el físico alemán Werner Heisenberg se dio cuenta de que las reglas de la probabilidad que gobiernan las partículas subatómicas nacen de la paradoja de que dos propiedades relacionadas de una partícula no pueden ser medidas exactamente al mismo tiempo. Por ejemplo, un observador puede determinar o bien la posición exacta de una partícula en el espacio o su momento (el producto de la velocidad por la masa) exacto, pero nunca ambas cosas simultáneamente. Cualquier intento de medir ambos resultados conlleva a imprecisiones.
Por lo tanto, la conclusión es que no es posible estudiar algo sin que ello conlleve alteración alguna. Lo que estudias, lo cambias. De ahí la importancia de que el perito siga una metodología que indique claramente que uno de los primeros y más importantes pases de la misma es trabajar con copias idénticas de las evidencias, preservando los originales para no modificarlos.
/El principio de Economia o la 'Navaja de Ockham'/

La navaja de Ockham (a veces escrito Occam u Ockam), principio de economía o principio de parsimonia (lex parsimoniae), es un principio metodológico y filosófico atribuido a Guillermo de Ockham (1280-1349), según el cual, en igualdad de condiciones, la explicación más sencilla suele ser la correc
Esto implica que, cuando dos teorías en igualdad de condiciones tienen las mismas consecuencias, la teoría más simple tiene más probabilidades de ser correcta que la compleja.
En el caso relativo a la investigación informática, la explicación más simple debería de ser la más sencilla de demostrar o descartar. Además, por la ley del mínimo esfuerzo, se debe de empezar a trabajar tomando inicialmente la hipótesis más sencilla.
Finalmente, en un plano más actual y más cercano a la realidad del día a día de un perito, encontramos que en la sección V, artículo 335 de la Ley 1/2000 de Enjuiciamiento Civil quedan recogidos los principios legales ante los que debe de responder un perito:

Artículo 335 Objeto y finalidad del dictamen de peritos. Juramento o promesa de actuar con objetividad:

1. Cuando sean necesarios conocimientos científicos, artísticos, técnicos o prácticos para valorar hechos o circunstancias relevantes en el asunto o adquirir certeza sobre ellos, las partes podrán aportar al proceso el dictamen de peritos que posean los conocimientos correspondientes o solicitar, en los casos previstos en esta ley, que se emita dictamen por perito designado por el tribunal.

2. Al emitir el dictamen, todo perito deberá manifestar, bajo juramento o promesa de decir verdad, que ha actuado y, en su caso, actuará con la mayor objetividad posible, tomando en consideración tanto lo que pueda favorecer como lo que sea susceptible de causar perjuicio a cualquiera de las partes, y que conoce las sanciones penales en las que podría incurrir si incumpliere su deber como perito.

3. Salvo acuerdo en contrario de las partes, no se podrá solicitar dictamen a un perito que hubiera intervenido en una mediación o arbitraje relacionados con el mismo asunto.

El informe pericial

Por injusto que parezca, ya que la carga técnica que implica la correcta resolución de una investigación forense resulta claramente abrumadora, al igual que sucede en un proyecto de auditoría, el valor del trabajo realizado en una investigación informática forense reside en la documentación entregada, ya que es el lugar donde se recoge el resultado y la información de todo el proceso.
Aunque los resultados hayan sido obtenidos legal y profesionalmente, siguiendo mejores prácticas y técnicas adecuadas para preservar la cadena de custodia, si en su fase final éstos no son adecuadamente documentados, es posible que no tengan ningún valor.
El informe pericial es el elemento de juicio fundamental respecto de la labor del investigador forense. Por lo tanto constituye, si no el más importante, uno de los elementos esenciales en un caso forense.
Para afrontar el desarrollo de un informe pericial hay que tener presente que:

- El objetivo final es transmitir información objetiva y clara, sin desestimar datos técnicos pero con la mínima carga tecnológica, y sin que ello implique una pérdida de rigor en la información presentada.

- Es necesario dejar patente la condición de independencia del perito.
- Normalmente el consumidor de la información son meros usuarios tecnológicos (jueces, abogados).
    - El informe debe de ser comprensible.
    - Para una persona sin conocimientos de informática, comprender aspectos tan básicos como el de dirección IP, puede suponer un problema.
    - Particularmente, el abogado debe de ser capaz de conocer y comprender la información esencial contenida en él.
- El informe no es una demostración de las capacidades técnicas del perito.
- Es necesario utilizar métodos pedagógicos para facilitar su comprensión.
- El informe no debe estar condicionado, y en ningún caso debe recoger otra información que no sean los resultados objetivos obtenidos durante la investigación.
- El informe debe presentar una línea maestra bien definida.
- Los objetivos iniciales deben de estar alineados con el desarrollo del informe pericial.
- La información recabada debe de justificar cuestiones relativas a la resolución del caso.
- El informe no puede presentar cuestiones no resueltas adecuadamente.
- El informe forense debe seguir a una estructura documental claramente definida.
- Pueden ser varios los modelos y apartados incorporados en el informe y se verán en el capítulo de buenas prácticas.

Más adelante se verá el tema del informe en detalle, tomando referencias de estándares internacionales y buenas prácticas.

Capítulo 4: ARTEFACTOS Y EVIDENCIAS DIGITALES

Artefactos

Cuando se afronta una investigación forense puede suceder que, en función de los datos facilitados por el cliente, no se encuentren 'pistas' claras y se requiera de uno o varios vectores de análisis menos evidentes para tratar de identificar evidencias. En estos casos uno de los pasos a dar es pelear con los rastros que deja el sistema operativo y aplicaciones .
Los artefactos son procesos o mecanismos de registro de los sistemas operativos y aplicaciones que dejan rastro de la actividad del sistema y de los usuarios, de los binarios que se utilizan, los accesos, conexiones, navegación, descargado o ejecutado algún programa entre otros aspectos.
El término artefacto es utilizado en la informática forense, aunque no existe una definición oficial de este término ni documentación profusa alrededor del mismo.
Dentro del ámbito informático, dicho término no debe confundirse con el término artefacto utilizado en el desarrollo de software.
La definición más cercana al significado de la palabra dentro de la informática forense es el de la palabra artefacto dentro de la arqueología.
Los artefactos pueden ser identificados en distintas localizaciones y, en el caso de Windows, podemos identificar artefactos en:

- Logs o ficheros de sistema.
- El registro de Windows.
- El visor de eventos.
- Tabla maestra de ficheros MFT.
- Los ficheros `prefetch`.
- Los accesos directos.
- Metadatos en imágenes y documentos.
- Ficheros de hibernación y memoria.
- Copias de seguridad y `volume shadow`.
- Ficheros descargados.
- Ejecución de programas.
- Creación y apertura de archivos.
- La papelera o eliminación de archivos.
- USB y dispositivos.
- Uso de cuentas.
- Uso de navegadores.

En los distintos libros que he leído y en la información utilizada para preparar el trabajo no he encontrado apenas referencias a los artefactos, sin embargo, en mi opinión son un concepto relevante dentro de contexto de una investigación forense, y es por ello que se referencian los mismos.
En mi opinión es evidentemente la necesidad de conocer o disponer de un listado de artefactos a la hora de enfrentar una investigación forense y, se identifiquen o no evidencias 'claras', introducir en la

metodología de base el tratamiento de los artefactos que pueden aportar información a la investigación decisiva a la hora de llegar a conclusiones.
Por otro lado, no es objeto de este proyecto fin de carrera identificar cada uno de los distintos artefactos de sistemas operativos o aplicaciones.

La evidencia digital

A mi entender y tras analizar distintas fuentes, una evidencia es cualquier elemento que permite sustentar, 'sin lugar a dudas', una conclusión frente a unos hechos determinados. El uso del entrecomillado se debe a que, en muchas ocasiones, una evidencia por si sola no permite sustentar una conclusión rotunda, sin embargo, la sinergia entre varias evidencias puede ser concluyente.
Pero, ¿un elemento que no permita ser concluyente se puede considerar evidencia?
Una evidencia (del latín, vídeo, ver), según wikipedia, es un conocimiento que se nos aparece intuitivamente de tal manera que podemos afirmar la validez de su contenido, como verdadero, con certeza y sin sombra de duda.
Sin embargo, evidencia, según la RAE, se define como:

> (Del lat. evidenta).
>
> 1. f. Certeza clara y manifiesta de la que no se puede dudar.
>   *La evidencia de la derrota lo dejó aturdido.*
> 2. f. Der. Prueba determinante en un proceso.

Desde el concepto de la evidencia en la filosofía tradicional hasta el actual ha habido diferentes interpretaciones. En mi opinión, el punto de inflexión se dio en la edad moderna, momento en el que los racionalistas y empiristas reconocieron la evidencia formal y su consistencia en sentido epistemológico (del griego episteme, 'conocimiento', y logos, 'estudio') en la deducción a partir de unos principios considerados evidentes, considerando que las deducciones son evidencias sucesivas de tipo formal según las leyes lógico-matemáticas, como relación de ideas. Hoy dicho procedimiento se concibe bajo el concepto de *análisis*.
Como 'dijo' Sherlock Holmes: '*Datos, datos, datos. No puedo fabricar ladrillos sin arcilla*'.
Obtener evidencias es fundamental a la hora de afrontar un análisis forense. El analista debe poder defender y contar con el principio de independencia a lo largo de todo el proceso, por lo que las buenas prácticas y metodologías son fundamentales para no invalidar las mismas.
Sin elementos digitales que analizar no puede existir el análisis digital. Sin embargo, tal como se puede extraer de su definición, no todos los elementos analizados durante una investigación se pueden considerar evidencias.
La prudencia es crítica cuando se sospecha que un activo de la empresa ha sido utilizado como medio para perpetrar una acción ilícita y que debe ser objeto de análisis.
Inicialmente debe asumirse que es posible que el activo contenga evidencias y por ello hay que tratarlo como un sistema con información importante y sensible para el caso. En muchos casos, las acciones siempre bien intencionadas de áreas como sistemas o desarrollo modifican el escenario sin las debidas medidas que deben de ser tomadas para manipular evidencias, lo que permite que, durante el juicio, que la parte interesada pueda alegar que las evidencias pueden haber sido manipuladas con el objetivo de favorecer o incriminar a alguien. Este es también habitualmente un argumento frecuentemente utilizado en análisis contrapericiales.
Adicionalmente, la información proporcionada por el personal afectado es crucial debido a los factores temporales y relativos a su localización. El analista es un ser humano, y uno de los mayores riesgos que debe de evitar en el inicio de un análisis forense es que sus capacidades se vean afectadas por la visión de los hechos relatada por dicho personal. Por lo que, en resumen:

- Los testimonios del personal afectado no debe de condicionar en modo alguno al analista.
- En ningún caso el analista debe seguir un impulso por llegar a obtener conclusiones que le haga actuar sobre las infraestructuras afectadas sin respetar el procedimiento adecuado para ello.

La evidencia digital, o prueba documental:

- Es la información relevante que permite a un analista establecer los motivos y fundamentos en los que se basan sus conclusiones.
- Se puede presentar como medio de prueba.
- Consiste básicamente en información digitalizada, codificados y alojados en un elemento contenedor digital (equipos, dispositivos periféricos, unidades de memoria, unidades virtualizadas, tramas de red y otros). Su valor es independiente del:
    - Formato de la misma (la codificación que permite guardar, tratar, recuperar o almacenar la información).
    - Dispositivo físico o virtual en el cual se encuentra contenida.
- Puede encontrarse en distintos estados que requieren procedimientos y herramientas distintas para garantizar la integridad de la misma:
    - Almacenada estáticamente en un contenedor digital.
    - Almacenada dinámicamente o en procesamiento en un elemento volátil.
    - En movimiento por la red en forma de trama de información que puede ser capturado y almacenado.
- Nunca debe de ser tratada directamente.
    - Se debe de realizar una copia bit a bit de modo que ésta sea idéntica a la original original, y sin alterar la integridad de la información original ni contaminarla
    - La copia puede ser copiada tantas veces como se precise, con métodos que garantizan que se está accediendo a la información en modo único de lectura, evitando su contaminación o modificación, la que permite desde el punta de vista de la cadena de custodia preservar integro el valor probatorio del original.

La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil establece en el capítulo V, 'De la prueba: disposiciones generales', en su:

- SECCIÓN 3: 'DE OTRAS DISPOSICIONES GENERALES SOBRE PRÁCTICA DE LA PRUEBA', expone que:
    - Las pruebas se practicarán en vista pública, si bien, excepcionalmente, el Tribunal podrá acordar, mediante providencia, que determinadas pruebas se celebren fuera del acto de juicio o vista.
    - Será inexcusable la presencia judicial en el interrogatorio de las partes y de testigos, en el reconocimiento de lugares, objetos o personas, en la reproducción de palabras, sonidos, imágenes y, en su caso, cifras y datos, así como en las explicaciones impugnaciones, rectificaciones o ampliaciones de los dictámenes periciales.

- Se llevarán a cabo ante el Secretario judicial la presentación de documentos originales o copias auténticas, la aportación de otros medios o instrumentos probatorios, el reconocimiento de la autenticidad de un documento privado, la formación de cuerpos de escritura para el cotejo de letras y la mera ratificación de la autoría del dictamen pericial, siempre que tengan lugar fuera de la vista pública o el Secretario judicial estuviera presente en el acto. Pero el Tribunal habrá de examinar por sí mismo la prueba documental, los informes y dictámenes escritos y cualesquiera otros medios o instrumentos que se aportaren.

Así como en su capítulo VI, 'De los medios de prueba y las presunciones', en su:

- SECCIÓN 8: 'DE LA REPRODUCCIÓN DE LA PALABRA, EL SONIDO Y LA IMAGEN Y DE LOS INSTRUMENTOS QUE PERMITEN ARCHIVAR Y CONOCER DATOS RELEVANTES PARA EL PROCESO', expone:

  - Que una de las evidencias o medios de prueba que se podrá hacer uso en un juicio es el 'dictamen de peritos'.
  - Que se admitirán, conforme a lo dispuesto en la Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.
  - Que las partes podrán proponer como evidencia la reproducción de palabras, imágenes y sonidos, captados mediante instrumentos de filmación, grabación o semejantes.
  - Que el tribunal, a instancia de parte, admitirá como prueba adoptando las medidas que en cada caso resulten necesarias, cualquier otro medio de prueba no expresamente previsto en los apartados anteriores, que permita obtener certeza sobre hechos relevantes.
  - La posibilidad de que las partes puedan aportar evidencias para cuestionar la autenticidad o exactitud de lo reproducido o mostrado.
  - La importancia de mantener las evidencias libres de posibles alteraciones y custodiadas adecuadamente.

Por lo que se puede concluir, que el condicionante para que un elemento sea considerado como evidencia, es que sea relevante para el proceso y útil para la acción probatoria de los hechos que se presentan.
Esto permite que cualquier tipo de registro o elemento que pudiese generarse en el futuro a causa del desarrollo tecnológico pueda ser considerado como evidencia si se demuestra su relevancia como tal.
En un juicio, la responsabilidad última de interpretación atiende al criterio del juez, que interpreta las leyes y las aplica según su entender. Por lo tanto, en relación con el tratamiento de las evidencias, sean cuales fueren los procesos y acciones llevadas a cabo por el analista, éstas serán validadas y refrendadas exclusivamente por él.
Pero finalmente, teniendo en consideración lo expuesto hasta el momento, llegará la hora de adquirir las evidencias como fase crítica del proceso. En este momento vuelve a aparecer la cuestión fundamental, ¿cuál es el procedimiento adecuado? De nuevo la respuesta es compleja, no existe un procedimiento único, así como tampoco existen unas herramientas 'validadas' y que sirvan específicamente a efectos judiciales.
La realidad es que a día de hoy no existe regulación en relación al tratamiento de evidencias. Sin embargo, existen una serie de buenas prácticas que serán tratadas en un capítulo posterior, así como normas no escritas cuyo seguimiento y aplicación es recomendable.
En muchos países de la Unión Europea, entre ellos España, no existe una legislación para la investigación forense digital. Si bien existen iniciativas de asociaciones de peritos como ASPEI, que desarrolla el

proyecto Konfía, no puede expresarse de forma taxativa qué proceso es el adecuado ni cuáles son las herramientas necesarias y cómo deben utilizarse.
Como se verá en detalle en el capítulo relativo a buenas prácticas, una operación crítica para el investigador forense es la copia de los soportes probatorios. A grandes rasgos, el proceso de copiado debe de garantizar que las copias realizadas deben ser idénticas al original y que éste no ha sido alterado. Igualmente, las buenas prácticas deben de disponer de medidas para garantizar que las conclusiones a las que se llega tras el análisis de las copias realizadas de las evidencias, parten de un soporte idéntico al original y por lo tanto no ha habido una manipulación del mismo.

Prueba anticipada

Durante una investigación forense digital es muy común que las evidencias necesarias para llegar a una conclusión se encuentre en manos de terceros, como proveedores de comunicaciones, fuera del alcance del perito. En relación con este tipo de situaciones se debe de tener en cuanta que:

- La obtención de las evidencias puede permitir identificar la motivación de un hecho o incriminar a una persona concreta en el proceso de investigación.
- Las posibles reflexiones que pueda realizar el analista no tienen validez dentro del proceso judicial.
- Es importante tener en consideración la volatilidad de estas evidencias.

Por éstas razones, entre otras, es recomendable agilizar la solicitud de acceso a dichas evidencias al órgano competente.
Este procedimiento se denomina solicitud de prueba anticipada, y está justificado en situaciones excepcionales que pueden amenazar la prueba misma o su calidad. La prueba anticipada no hace sino reconocer y plasmar en el caso particular el derecho a probar que corresponde esencialmente a las partes y que es propio del debido proceso.
Un caso claro de prueba anticipada y que ya he vivido en varias ocasiones debido a mi implicación en investigaciones forenses, es la necesidad de solicitar datos concretos relativos a una dirección IP a un proveedor de comunicaciones. Ésta información sólo puede ser solicitada mediante orden judicial a solicitud de un órgano competente como puede ser la policía.
Los artículos 293 a 298 de la sección IV de la Ley 1/2000 de Enjuiciamiento Civil recogen el ordenamiento de la prueba anticipada.
Aunque la institución de la prueba anticipada se parece a otras como, por ejemplo, la *prueba preconstituida* o *prueba para perpetua memoria*, tiene características particulares que la convierten en una institución diversa de ellas.
Esto implica que, aunque el proceso judicial no haya sido iniciado, cualquiera de las partes puede solicitar que se practique el proceso de solicitud anticipada, debiendo ser motivado y solicitado al tribunal que está llevando el caso siempre con anterioridad al inicio del juicio.
Si bien el escrito de solicitud, mediante una súplica de oficio, es remitido por el abogado que lleva el caso ante el juzgado correspondiente, es recomendable que el escrito sea revisado por el analista forense con el fin de asesorar al abogado y evitar con ello incurrir en errores técnicos que hagan imposible atender a la súplica.
Para el caso de un procedimiento de solicitud de prueba anticipada en el que se solicite información, a una empresa de comunicaciones, acerca del propietario de una línea, éste deberá de complementarse con el máximo de información posible. En este caso, se deberá de facilitar en la solicitud:

- El proveedor asociado a la línea.
- Dirección IP o dominio de la resolución inversa de la misma.

- Datos temporales concretos de conexión.

De forma que el procedimiento de solicitud pueda ser diligenciado eficientemente.
El analista forense deberá de tener en cuenta las posibles discrepancias temporales que pueden tener las trazas del escenario analizado, con las de los datos facilitados por el proveedor correspondiente.

La cadena de custodia

Como perito, la clave para afrontar un proceso judicial en las mejores condiciones, es garantizar la consistencia de las conclusiones presentadas mediante las evidencias digitales adquiridas. Este objetivo se consigue mediante la utilización de procesos, procedimientos y buenas prácticas que garanticen la no alteración de las evidencias.
El procedimiento de custodia de la evidencia o 'cadena de custodia', desde su identificación hasta su presentación debe de ser igualmente riguroso. La documentación es otro aspecto clave que afianzará la garantía de no alteración, crítica para el proceso de análisis forense.
Según la wikipedia, 'La cadena de custodia de la prueba se define como el procedimiento controlado que se aplica a los indicios materiales relacionados con el delito, desde su localización hasta su valoración por los encargados de su análisis, normalmente peritos, y que tiene como fin no viciar el manejo de que ellos se haga y así evitar alteraciones, sustituciones, contaminaciones o destrucciones'.
De esta forma se asegura que los elementos probatorios ofrecidos como evidencias o pruebas documentales informáticas, son confiables.
Es necesario establecer un riguroso y detallado registro, que identifique la evidencia y posesión de la misma, lugar, hora, fecha, nombre y dependencia involucrada, en la recolección o adquisición, la interacción posterior y su depósito en la sede que corresponda (judicial o no).
La buena noticia es que, en el caso de las pruebas y evidencias informáticas, se cuenta con una gran ventaja frente a otro tipo de evidencias o pruebas ya que, normalmente, es posible realizar copias idénticas de la evidencia de forma que se pueden realizar todas las pruebas y exámenes pertinentes para llegar a las conclusiones probatorias sin necesidad alguna de trabajar con las evidencias originales, evitando cualquier tipo de manipulación, daño o contaminación de las mismas.
El órgano competente debe poder confiar en la integridad de dichas evidencias por considerarlos "testigos mudos", desde el punto de vista criminalístico clásico, y evaluarlos en tal sentido.
Desde un punto de vista legal, nuestro ordenamiento jurídico sólo menciona la cadena de custodia, indirectamente, en el artículo 334 de la Ley de Enjuiciamiento Criminal, donde regula:

```
El Juez instructor ordenará recoger en los primeros momentos las armas,
instrumentos o efectos de cualquiera clase que puedan tener relación con
el delito y se hallen en el lugar en que éste se cometió, o en sus
inmediaciones, o en poder del reo, o en otra parte conocida. El
Secretario judicial extenderá diligencia expresiva del lugar, tiempo y
ocasión en que se encontraren, describiéndolos minuciosamente para que
se pueda formar idea cabal de los mismos y de las circunstancias de su
hallazgo.

La diligencia será firmada por la persona en cuyo poder fueren hallados,
notificándose a la misma el auto en que se mande recogerlos.
```

Así como en el artículo 338 LECrm, donde se especifica que se debe de garantizar su integridad, retención, conservación o depósito:

> Sin perjuicio de lo establecido en el Capítulo II bis del presente título, los instrumentos, armas y efectos a que se refiere el artículo 334 se recogerán de tal forma que se garantice su integridad y el Juez acordará su retención, conservación o envío al organismo adecuado para su depósito.

La cadena de custodia es un procedimiento que permite trazar y verificar todas las pruebas que se han realizado sobre cada una de las evidencias. El personal competente puede consultar en cualquier momento la ubicación de la evidencia en un momento dado, los diferentes analistas que han inspeccionado la evidencia, y así evitar la contaminación, alteración, posibles daños, reemplazos, contaminación o destrucción de las mismas.

No he encontrado regulación especifica para procedimentar y garantizar la custodia de pruebas, ni en España ni en otros países.

El Instituto Universitario de Investigación en Ciencias Policiales (IUICP) se inauguró el 19 de junio de 2007. Es una institución mixta que depende de la Universidad de Alcalá (UAH) y de la Secretaría de Estado de Seguridad del Ministerio del Interior y, que se dedica a la investigación científica y técnica y al desarrollo de programas docentes en materia policial.

Durante la celebración del IV Encuentro de Investigadores del IUICP se concedieron nueve proyectos cuyo contenido aparece en la MEMORIA IUICP 2010. Uno de los proyectos actualmente en curso, con código IUICP/PI2010/002, lleva por título 'La cadena de custodia como garantía de la evidencia probatoria. Propuesta de regulación normativa.'.

Para que las pruebas periciales practicadas se declaren plenamente válidas es imprescindible garantizar la corrección de la denominada "cadena de custodia". Su fin es asegurar que aquello que se presenta ante el Tribunal como evidencia es lo mismo que se encontró en el escenario delictivo. Sin embargo, y aunque la Ley procesal ya contenga algunas previsiones sobre el aseguramiento de las pruebas, al ordenar que se adopten las medidas necesarias para que su recogida y custodia se verifiquen en condiciones que garanticen su autenticidad, no existe una normativa expresa que regule las exigencias mínimas para garantizar formalmente la "cadena de custodia". Pese a ello, su existencia se asume por la comunidad jurídica y su garantía se reclama ante los Tribunales de Justicia.

Ante la citada falta de regulación, los expertos en Criminalística han ido elaborando unos protocolos de actuación internos, con el fin de documentar todas y cada una de las fases que recorre todo elemento probatorio, dejando constancia de cada uno de sus pasos, con el objetivo último de fortalecer lo que de ellos dictamine el experto en su informe pericial. A este proceder es al que se ha dado valor jurídico y se conoce como cadena de custodia policial.

Teniendo en consideración lo anterior, es necesario incorporar un fichero de cadena de custodia para cada evidencia existente.

No obstante, si se tienen en cuenta las últimas reformas de la LECrim, los citados protocolos de actuación policial, la jurisprudencia y algunas Recomendaciones del Consejo de Europa, podemos extraer que se ha construido un "corpus iuris " (Cuerpo de Derecho) que es asumido como vinculante por la comunidad jurídica.

Partiendo de lo anterior, el proyecto IUICP/PI2010/002 pretende conseguir una regulación normativa de la cadena de custodia policial, que contenga las formalidades, medidas y precauciones necesarias que deben adoptarse en cada una de las fases que recorre la prueba para que su recogida, custodia, traslado y análisis se verifique en las condiciones que permitan garantizar su corrección. Y todo ello teniendo en cuenta las características específicas de cada prueba, que puede dar lugar al empleo de diversos métodos en cada una de las fases de dicho procedimiento.

En definitiva, regular la hoja de ruta de la prueba, con el fin de garantizar la corrección del recorrido que sigue todo vestigio delictivo hasta convertirse en evidencia probatoria, reforzando así el derecho a un proceso con todas las garantías.

Me he puesto en contacto con la Profesora M. Carmen Figueroa Navarro, Profesora Titular de Derecho Penal de la UAH e Investigadora Principal del Proyecto IUICP/PI2010/002 antes mencionado para interesarme por el estado de la propuesta de regulación normativa, ya que he estado buscando información del actual estado del arte en relación con la cadena de custodia en España y he encontrado referencias a dicho proyecto, que me ha parecido muy interesante y algunas referencias al objetivo del proyecto, una entrevista y un artículo, no me ha sido posible localizar más información.
Muy amablemente la profesora Figueroa me contestó, a fecha 21 de junio de 2013, con el siguiente texto:

```
Estamos en la última fase de desarrollo del proyecto, aunque aun no se
ha concluido, y uno de los aspectos que se analizan en la parte jurídica
es precisamente la relacionada con la cadena de custodia de vestigios
electrónicos e informáticos, mediante el estudio de las sentencias de
los tribunales que han tenido en cuenta informes periciales informáticos
(sobre evidencias digitales) de los laboratorios forenses, donde se ha
alegado falta de aseguramiento en la cadena de custodia.

Efectivamente, en el marco del IUICP, estoy dirigiendo un proyecto de
investigación relacionado con la cadena de custodia, tanto desde un
punto de vista técnico como jurídico, para lograr una regulación
normativa sobre este tema.

Le adjunto dicho artículo, así como otros que tal vez puedan servirle
para su proyecto de fin de carrera.
```

En el artículo escrito y mencionado por la profesora se hace referencia a la necesidad de normalizar la cadena de custodia.
En relación con los informes periciales practicados sobre los soportes electrónicos o informáticos incautados, se ha alertado sobre la importancia que reviste en esta prueba la cadena de custodia en distintas ocasiones:

- Urbano Castrillo, E.: «La regulación legal de la prueba electrónica: una necesidad pendiente», en La Ley Penal, n.o 82, mayo 2011, pág. 13.
    - Ya que no se trata de pruebas inalterables o de difícil manipulación, sino, antes al contrario, pruebas que se denominan virtuales precisamente por su esencial alterabilidad en todo momento.
- Sanchís Crespo, C.: «La pericia informática en el proceso penal», en Revista de Contratación Electrónica, n.o 91, marzo 2008.
    - La importancia de la cadena de custodia es fundamental para garantizar la integridad de las evidencias informáticas que se presentarán después como prueba en un juicio. Una mala praxis en los momentos iniciales frustrará por completo la investigación.
- Velasco Núñez, E.: «ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal», en La Ley Penal, n.o 82, mayo 2011, pág. 25.
    - Se ha señalado que la aportación al proceso de sus resultados incriminatorios se efectúe 'de la manera más auténtica y fiable posible, garantizando su genuinidad, e inmodificabilidad a la hora de probar su existencia y a la de trasvasar a soportes más manejables los datos que precise conocer, tanto la acusación como la defensa, que garanticen de forma fiable que no se han operado cambios sustanciales'.

- Insa, F./Lázaro, C.: «La admisibilidad de las pruebas electrónicas en los tribunales (APET): Luchando contra los delitos tecnológicos», en Diario LA LEY, de 8 de mayo de 2007.

    - Los requisitos técnicos formales que se incumplen más habitualmente en Europa son los relativos al cumplimiento de las medidas necesarias para la comprobación de la autenticidad y la inalterabilidad del documento electrónico, del correo electrónico enviado así como la falta de firma electrónica en documentos que quedan sin fuerza probatoria a la hora de ser presentados

Esta norma, una vez propuesta y aplicada, deberá tenerse en consideración para la cadena de custodia policial por parte de las diferentes unidades de las fuerzas y cuerpos de seguridad del estado.
Sin embargo, aunque puede ser tomada como referencia, no afectará a aquellos análisis que sean realizados en el ámbito privado.
Es muy normal que, a lo largo de un análisis, tanto las evidencias como las copias garantizadas de las mismas sean compartidas entre distintos analistas y otras organizaciones involucradas en el proceso.
El compromiso y responsabilidad del mantenimiento del procedimiento adecuado de la cadena de custodia de las evidencias es trasladado al tenedor de la misma, quedando todo el procedimiento registrado. La cadena de custodia permite identificar con claridad quién ha estado en posesión de las evidencias antes de que éstas sean utilizadas en instancias judiciales, permitiendo que cualquier depositario de las mismas pueda ser citado judicialmente si las evidencias quedaran en entredicho durante el proceso.
Como puede extraerse, la cadena de custodia permite al analista garantizar la independencia y objetividad en la elaboración de sus conclusiones, y demostrar que no se ha realizado manipulación alguna de las evidencias para favorecer a una de las partes.
Es por ello que la cadena de custodia deber recoger en todo momento información que permita contestar a las siguientes cuestiones:

- ¿Quién es el depositario?
- ¿Fecha y hora de entrega? ¿Durante qué espacio temporal lo es?
- Si se ha desplazado ¿dónde se localiza?
- ¿Cuál es la razón por la que la evidencia queda bajo su custodia?
- ¿Qué medidas se han tomado para su conservación y protección?

No me ha sido posible identificar la existencia de un modelo de fichero homologado de cadena de custodia o de uso generalizado. He localizado en la red un gran número de formularios de distintas entidades, tanto públicas como privadas, que pueden ser válidos. Además, varias de las herramientas forenses de adquisición de evidencias disponen de sus propios modelos, como es el caso de FTK. Finalmente, si se recoge la información necesaria, es posible generar el fichero de forma manual, tal y como se hará en este PFC.
Lo relevante es contar con algún archivo de cadena de custodia asociado a la evidencia y que contenga la información de identificación imprescindible.
El archivo de cadena de custodia es, en esencia, un formalismo, pero como tal es parte esencial del proceso. Si bien es posible que nunca sea requerido en el proceso judicial, en otros casos puede ser crítico para resolver dudas sobre las evidencias que alguna de las partes puede intentar fomentar en beneficio propio.

Intervención del Fedatario Publico en la Cadena de Custodia

El Fedatario Publico, que según el caso puede ser un notario o un secretario judicial, es clave para el aseguramiento de la Cadena de Custodia e interviene en las actuaciones forenses dando fe de lo sucedido durante el proceso de identificación.
Desde el punto de vista de la Cadena de Custodia el fedatario es necesario para que se cumplan varias funciones críticas relativas a la veracidad e integridad de algunos de los principales procesos forenses ejecutados durante la investigación.

- Función descriptiva

  El fedatario publico ha de dar fe de la correcta descripción de:

  - El escenario en el cual se está llevando a cabo la actuación forense: entorno, condiciones, contexto, ubicación, localización y cualquier información que se considere relevante, apropiada, curiosa o significativa.
  - Los bienes identificados: condiciones, elementos, dispositivos y cualquier información que se considere relevante, apropiada, curiosa o significativa.
  - Los actores que intervienen directa o indirectamente: quien, rol que desempeña, relaciones, actuación que realiza, y cualquier información que se considere relevante, apropiada, curiosa o significativa.

- Función registral e identificativa

  El proceso de identificación implica la recopilación, por parte de los analistas, de la información y de evidencias necesarias susceptibles de contener evidencias, para su posterior análisis y, paralelamente, construir un registro detallado, exhaustivo y completo de este material.

  El fedatario publico da fe tanto del contenido de la lista de registro e identificadores de las evidencias recopiladas, como de las copias de las evidencias que han sido puestas a disposición del órgano competente para su custodia y preservación.

- Función de validación del procedimiento

  El fedatario publico da fe de cómo se realiza los procesos de identificación y recopilación de la información para mitigar cualquier duda al respecto de cómo se han realizado las actuaciones, y que podrían anular la evidencia.

  Esto se debe a que la evidencia digital puede ser fácilmente:

  - Manipulada por los expertos conocedores de la materia.
  - Contaminada accidentalmente por la realización de un procedimiento u operación errónea.
  - Transgredida, al darse la situación en las que podrían verse violados los derechos concernientes a la confidencialidad de información personal del propietario de los dispositivos o evidencias.

  Ejemplos concretos de la labor del fedatario durante la investigación seria, dejar constancia y dar fe de que:

  - Los elementos en los cuales se vuelca la información recabada son adecuados: discos, CDs o DVDs nuevos que se desprecintan durante la actuación, memorias USB que se aportan en su embalaje original y, en caso de que no sean nuevos, que sean sanitizados adecuadamente (HARDWIPE).

- Se han realizado la cantidad de copias expresadas por el analista, que cada una de ellas está identificada adecuadamente y que está documentado su destino y el receptor de las mismas.
- El analista describe las actuaciones que se van a realizar y las ejecuta en presencia del fedatario, para que el mismo de fe de que no ha habido ninguna manipulación mas allá de las relatadas y de las que constan en el informe del analista.
- El analista, a pesar de no haber encontrado ninguna evidencia relativa a unos conceptos específicos identificadas de antemano, ha buscado una lista de palabras claves en los ficheros de un determinado equipo.

- Función de validación de la correcta transmisión de la custodia

  En todo análisis forense se producen transmisiones de la custodia de entre distintas partes habilitadas para el tratamiento de las evidencias. Para la correcta ejecución de dicho procedimiento se requiere disponer de un registro con la información relevante, que seria: qué se transfiere o entrega, cómo esta identificado, cuantía o cantidad, quien hace la entrega, quien la recibe, donde se realiza, cuando, en que condiciones, y cualquier información que se considere relevante, apropiada, curiosa o significativa.

  El fedatario debe dar fe del correcto proceso de transmisión, puesto que ello implica un cambio de la titularidad de la responsabilidad de custodia sobre la evidencia.

Capítulo 5: EMACS

¿Por qué Emacs?

Utilizo Emacs desde hace tiempo a nivel profesional y al plantearme las necesidades de un analista forense pensé en Emacs.
Es cierto que no se trata de la herramienta más intuitiva del mundo, ni la más bonita, ni la más fácil de aprender. Pero creo que la afamada frase 'menos es más' del arquitecto *Ludwig Mies van der Rohe* es la que mejor define a esta aplicación.
Podría explicar las razones por las que considero a Emacs una herramienta interesante a tener en cuenta para desarrollar un análisis forense, entre otras la facilidad para cifrar toda la información, pero creo que la mejor aproximación es ver su potencial a medida que desarrollo algunos de los comandos y secuencias de teclas que debería de conocer un analista para trabajar eficientemente. Además, como entiendo que al finalizar este capítulo cualquiera seguirá teniendo dudas al respecto, he desarrollado el 100 % del actual proyecto con ésta herramienta y al analizar en profundidad la totalidad del contenido del mismo, creo que será prueba suficiente de la idoneidad de Emacs como piedra angular a la hora de llevar a cabo un análisis forense (o cualquier otro proyecto).
Un editor de texto es un programa que permite crear y modificar archivos digitales compuestos únicamente por texto sin formato, conocidos comúnmente como archivos de texto o texto plano. El programa lee el archivo e interpreta los bytes leídos según el código de caracteres que usa el editor. Hoy en día es comúnmente de 7-bits ó 8-bits en ASCII o UTF-8.
No debe confundirse con procesador de texto o corrector de textos.
Emacs es un editor de texto con una gran cantidad de funciones, muy popular entre usuarios técnicos. Gnu Emacs (editor para desarrollar el presente PFC) es obviamente parte del proyecto GNU y la versión más popular de Emacs con una gran actividad en su desarrollo. El manual de GNU Emacs lo describe como 'un editor extensible, personalizable, auto-documentado y de tiempo real.'
El EMACS original significa, `Editor MACroS` funcionando en TECO (Text Editor and Corrector). Fue escrito en 1975 por Richard Stallman junto con Guy Steele. Hay muchas versiones de EMACS hasta el momento, pero actualmente hay dos que son usadas comúnmente: GNU Emacs, iniciado por Richard Stallman en 1984, y XEmacs, una fork de GNU Emacs, que fue iniciado en 1991. GNU Emacs es mantenido por el Proyecto GNU Emacs, el cual cuenta entre sus miembros a Richard Stallman.
Además, el modo Org (Org-mode) es un modo de edición de Emacs mediante el cual se editan documentos jerárquicos en texto plano. Su uso encaja con distintas necesidades, como:

- Registrar tiempos.
- Organizar tareas *TO-DO*.
- Hacer listas (checkboxes).
- Manejo de agenda y calendario.
- Planificar proyectos.
- Realizar documentos estructurados.
- Documentar código para ejecutarlo.
- Ejecutar código y que quede documentado.
- Manejar tablas y plantillas de cálculo.
- Trabajar con bases de datos.
- Hacer presentaciones.

- Registrar notas.

Por ejemplo, los elementos *TO-DO* (cosas por hacer) pueden disponer de prioridades y fechas de vencimiento, pueden estar subdivididos en subtareas o en listas de verificación, y pueden etiquetarse o darse propiedades. También puede generarse automáticamente una agenda de las entradas de cosas por hacer.
La mayor parte del comportamiento del modo Org puede personalizarse mediante los procedimientos habituales en Emacs (es decir estableciendo directamente el valor de las variables o utilizando la interfaz `Customize`, más amigable para los usuarios).
Desde la versión 22 de Emacs, el modo Org es parte de su distribución oficial - aunque también dispone de entregas separadas.
Un ejemplo de la sintaxis de Org-mode es:

```
* titulo [0/1] [0%]
** TODO una tarea con estado PORHACER   :un_tag:otro_tag:

   - *negrita*
   - /italica/
   - =codigo=
   - ~verbatim~

   Parrafo de texto medio corto.

   - [-] lista por completar [1/2] [50%]
         - [X] item que est  completo
         - [ ] item por realizar
```

Si se edita este fichero en formato org desde un procesador de textos, se observan construcciones del tipo `#+BEGIN_SRC` y `#+END_SRC`. Este tipo de constructores permite trabajar desde la plataforma propuesta con bloques de código de distintos lenguajes con Org mode, ejecutar los mismos o componer, como se verá más adelante, ficheros de código completos al mismo tiempo que se escribe la documentación relativa al mismo, con la facilidad de que, en cualquier momento, se pueden obtener ambos contenidos por separado. Eso es lo que se conoce como `programación literaria`.
La ampliación de capacidades de Org mode relativas al uso de código viene implementada por Babel, del que se hablará en distintos momentos en el actual capítulo.
Antes de empezar a explicar algunos keystrokes creo que es importante tener un mínimo de cultura general de Lisp (list processing), ya que está totalmente relacionado con Emacs (más de un 75 % está escrito en lisp, algo más de un 23 % en C, y el resto en lenguajes como sh, perl, awk, python y demás).
En primer lugar decir que Lisp es un lenguaje de programación multiparadigma, de alto nivel, declarativo, funcional, orientado a objetos y con 50 años de historia. La potencia de lisp es mucho mayor de la que lo gente piensa y aunque tiene relación con la IA (Inteligencia Artificial) se usa y se ha usado para muchísimas cosas más, como estudiar los paradigmas de los lenguajes de programación del futuro.
Lisp tiene 3 dialectos principales hoy en día (aunque existen más), éstos son `Scheme`, `Common lisp` y `Emacs lisp`.

- Scheme: la filosofía de Scheme es minimalista. Scheme proporciona un número muy reducido de primitivas, construyendo el resto a partir de este reducido número de abstracciones. El estándar (R5RS) tan sólo ocupa unas 50 páginas y se puede descargar de la página de schemers.org.

- Common lisp: por otro lado tenemos common lisp, el índice de las especificaciones de éste es tan grande como todas las especificaciones de scheme, por lo lo que posee un gran número de primitivas. La especificación y referencia más cercana es la CLtL.

- Emacs lisp: por último tenemos Emacs lisp, este dialecto fue escrito pensando u orientado para el entorno Emacs. El juego de primitivas que ofrece no es tan pequeño como el de Scheme, pero tan poco tan grande como el de Common lisp. Su número de primitivas también es reducido, lo que ocurre es que el estándar también define la biblioteca, que se construye con el juego de primitivas reducidas.

Finalmente, comentar que Emacs, además de exportar a distintos formatos como HTML, dispone de la capacidad de ejecutar un servidor HTTP para visualizar los contenidos desarrollados y exportados adecuadamente.

Emacs: Conocimientos mínimos para enfrentar un análisis forense

Es cierto que la curva de aprendizaje de Emacs no es precisamente ágil, y que los inicios pueden ser un poco complicados. Sin embargo, todo lo que merece la pena tiene un coste, y en este caso se trata de dedicarle tiempo y ser constante.
Para facilitar el proceso de aprendizaje, en el capítulo de anexos se describen los conocimientos y comandos comúnmente más utilizados en el desarrollo de una investigación forense. Los puntos desarrollados son:

- Convenciones
- Ayuda de Emacs
- Configuración inicial
- Comandos básicos
- Ventanas
- Copiar, cortar, insertar y borrar
- Buscar y reemplaza
- Formato de texto
- Tablas
- Listas
- Tareas
- Marcas
- Propiedades
- Columnas
- Enlaces
- Imágenes
- Gestión del tiempo
- Extensiones de ORG
- Cifrado de información
- Bloques de código
- Exportar a

Programación literaria

¿Qué es la programación literaria?

Tal como se explica en wikipedia, la programación literaria es un paradigma de programación propuesto por Donald Knuth como alternativa al paradigma de programación estructurada en la década de 1970.
El paradigma de programación literaria permite desarrollar programas en el orden fijado por la lógica y el flujo de pensamientos humano, obviando el orden impuesto por los sistemas informáticos y obviando la necesidad de tener en cuenta las restricciones impuestas por los lenguajes de programación tradicionales.
Un programa se desarrolla como una explicación de la lógica del mismo expresado en lenguaje natural, intercalando fragmentos de código fuente tradicional oculto tras macros.
El objetivo de la programación literaria es, por un lado, facilitar el entendimiento del programa desarrollado mediante la descripción en lenguaje humano de la lógica asociada a los fragmentos de código fuente desarrollados. Y paralelamente separar el programa propiamente dicho de tal forma que pueda ser compilado y ejecutado.
La primera generación de herramientas de programación literaria estaban centradas en un lenguaje de programación específico, sin embargo, las últimas son independientes del lenguaje y se sitúan por encima de los lenguajes de programación.
Según su ideólogo, la programación literaria permite desarrollar programas de mayor calidad ya que obliga a los programadores a documentar de manera natural la lógica del programa, lo que permite identificar con mayor facilidad aspectos como malas decisiones de diseño, replantear fácilmente sus propios procesos de pensamiento en cualquier momento posterior, y a los programadores que tienen que trabajar sobre el código en cualquier momento posterior, sin necesidad de consultar al autor del mismo, les posibilita entender la construcción y lógica del programa con mayor facilidad. Esta forma de trabajar difiere de la documentación tradicional (cuando la misma existe), en el que el programador presenta un código fuente que sigue el orden impuesto por el compilador, y debe descifrar el proceso de pensamiento detrás del programa a partir del código y sus comentarios asociados.
Sin embargo, no hay que confundir la programación literaria con la documentación producida a partir de un formato de archivo común tanto con el código fuente y los comentarios, o voluminosos comentarios incluidos en el código. La programación literaria, por ejemplo, implementa la 'red de conceptos abstractos' asociados al sistema de macros de lenguaje natural y proporciona la capacidad de cambiar el orden del código fuente de una secuencia de la máquina-impuesta a una vista cómoda para la mente humana.
Existen diferentes herramientas que implementan las bases funcionales de la programación literaria, sin embargo no es objetivo de este proyecto profundizar en esta línea de conocimiento.

¿Por qué utilizar la programación literaria?

La documentación, en cualquier formato representada, es una de las fuentes de información más importantes.
Centrándonos en el proceso mental asociado a la actividad forense que aborda el proyecto uno de los factores críticos es disponer de la posibilidad de replicar de la forma más objetiva y pragmática posible el proceso, pruebas y resultados de la investigación llevada a cabo.
Si bien es cierto que la labor de investigación se desarrolla a partir de metodologías previamente documentadas, no es menos cierto que cada investigación es singular en sí misma y el detalle de cada una de ellas es distinto.
A la hora de documentar las acciones realizadas es importante describir la metodología seguida, sin embargo, la posibilidad de explicar en detalle y, por decirlo de alguna forma, 'en tiempo real' cada una de las acciones planteadas asociadas al proceso mental y al contexto, creo que aporta un valor adicional a cualquier resultado obtenido durante la investigación.

Adicionalmente, la programación literaria permite desarrollar la estructura de carpetas en tiempo real, ya que permite crear las mismas sobre la estructura documental. Esto es, permite generar no sólo los ficheros de documentación, configuración, código y cualquier otro que sea necesario, sino que es posible almacenarlos en las estructura de carpetas que se desee aunque las mismas no estén creadas.
El sistema de marcas (markup) es muy ligero, pero incluso más potente que *Markdown* y más claro que *sRT*.
La estructura de edición de Org permite organizar cualquier tipo de información muy rápidamente y de forma muy clara. Y el control de versiones de ficheros Org es muy sencillo utilizando sistemas como GIT.
Org permite, de forma muy sencilla, editar documentos y exportarlos a formatos como HTML (para blogs) o LaTeX siguiendo la máxima *write-once, express-many-times*, que expresa la facilidad con que se exportan los documentos tras ser modificados.
En relación a las facilidades a la hora de codificar, Org permite una gran granularidad en forma de bloques de código. Estos bloques pueden ser identificados individualmente y ser referenciados desde otros, ser evaluados o no (ejecutados), mandar datos o exportar los mismos, especificar distintas sesiones REPL y, como se ha comentado, crear distintos ficheros en los que se distribuye el código e información a criterio del usuario. Los bloques permiten identificar visualmente la sintaxis del código utilizado y ser editados fácilmente en un modo mayor asociado el lenguaje de programación utilizado. Adicionalmente, cada fichero org permite desarrollar bloques de código en distintos lenguajes sin que ésto suponga ningún problema.
El meta-desarrollo planteado gestiona toda la complejidad del mismo desde una perspectiva de coherencia: el hecho de utilizar un fichero unificado permite el un acercamiento holístico al desarrollo global, que no se queda en la idea de desarrollar documentación y código de forma natural sino que abstrae el ciclo completo y unificado del desarrollo de la documentación requerida en la investigación.

Aplicación práctica sobre Emacs

Los prerequisitos para utilizar la programación literaria como modelo para el desarrollo de la documentación y codificación de un entregable en función de las premisas que aplican sobre el desarrollo del proyecto son disponer de:

- Una versión reciente de Emacs, 24.3+.
- Paquetes relativos a los lenguajes de programación a utilizar.
- Org-mode (incluido en la distribución de Emacs por defecto a partir de la versión 24).

Es muy recomendable, tal como se ha comentado anteriormente, utilizar algún paquete como Emacs Starter Kit, Emacs Prelude o Emacs Live.

- Notación de los bloques de código

  En el apartado anterior se han descrito de forma básica los bloques de código.

  El funcionamiento básico de la programación literaria utilizando Emacs se puede resumir en una serie de conceptos paramétricos y reglas a la hora de trabajar con los bloques de código.

  En la web de Org hay información acerca de la forma correcta de trabajar con código fuente, y a continuación he desarrollado algunas de las propiedades, funciones y argumentos más relevantes a la hora de disponer de una serie de conocimientos mínimos.

```
#+PROPERTY: mkdirp yes
#+PROPERTY: tangle proyecto.py
```

#+PROPERTY: mkdirp yes es una propiedad, que aplica a nivel global un argumento, que especifica que se permite crear la estructura de directorio en la que se crean los ficheros de código, lo que es interesante a la hora de desarrollar distintos ficheros en sus correspondientes directorios.

#+PROPERTY: tangle proyecto.py es una propiedad, que aplica a nivel global un argumento relativo a 'tangling', término adoptado de la comunidad de programación literaria, hace referencia a la creación de ficheros de código mediante la extracción del mismo de los bloques de código de un documento. Está directamente relacionado con la propiedad anterior ya que, en caso de especificarse la primera, tras el argumento

Otra forma de aplicar los anteriores argumentos a nivel de bloque de código es:

```
#+BEGIN_SRC python :mkdirp yes :tangle proyecto.py
  def times_two(x):
       y = x*2
       return y

  print times_two(5)
#+END_SRC
```

:mkdirp argumento que especifica si se permite la creación de la estructura de directorios en el momento de la exportación. Anteriormente se ha visto su uso estableciéndolo como propiedad del fichero.

:tangle es otra forma de especificar el argumento `tangle` para especificar el fichero de código por defecto. Se especifica el PATH y el nombre del fichero a crear. Por defecto su valor es `no`, por lo que el bloque de código no será tratado.

Otros argumentos específicos de la cabecera de los bloques de código son:

:var pasa argumentos variables a los bloques de código (`:var x=2`).

:results especifica el tipo de resultados, y como serán recolectados y tratados.

:session permite, una vez especificado un nombre de sesión, establecer la misma e incluso varias concurrentes para cada lenguaje interpretado.

:noweb especifica si se expanden las referencias noweb cuando el bloque de código es evaluado, exportado o tangled.

:cache evita volver a calcular los bloques de código que no han sido modificados.

:file permite especificar un fichero para que almacene el resultado de la ejecución del bloque de código.

:dir especifica el directorio por defecto (posiblemente remoto) para la ejecución del bloque de código.

:exports indica, en caso positivo, si se exporta el código, los resultados o ambos.

:shebang indica si el código se guarda en ficheros ejecutables.

:tangle-mode permite establecer los permisos de los ficheros generados (tagled).

:eval normalmente se utiliza como medida de seguridad a la hora de evaluar bloques de código potencialmente peligrosos.

:wrap ese utiliza para marcar los resultados de la evaluación bloque de origen.

:post se utiliza para el procesamiento posterior de los resultados de bloques de código.

:comments gestiona inserción de comentarios en ficheros de código exportados(tangle).

:padline controla la inserción de líneas (padline) entre los bloques de código exportados.

:no-expand permite evitar que los bloques de código se expanden con org-babel-expand-src-block durante la exportación (tangle). Esto tiene como efecto la NO asignación de valores a las variables especificadas con `:var`, y la NO sustitución de las referencias 'noweb' con sus objetivos.

:org-babel-expand-src-block es la función que expande los bloques de código ya sean variables o referencias de estilo 'noweb'.

Ejemplo práctico

Un ejemplo del uso de la programación literaria utilizando algunos de los argumentos anteriormente es el siguiente bloque de código:

```
#+NAME: gpgFilesToPDF
#+BEGIN_SRC emacs-lisp :exports code :mkdirp yes :tangle ~/.emacs.d/gpgFilesToPDF.el
(defun gpgFilesToPDF (buf1 buf2 file_name)
    (interactive 'bFichero de MACROS: \nbFichero BASE: \nsNombre del fichero PDF: ')
        ; create a new 'tempBuf' buffer
        (let ((myBuf (get-buffer-create 'tempBuf')))
            ; make it the current displayed buffer
            (switch-to-buffer myBuf)
            (insert-buffer-substring buf1)
            (insert-buffer-substring buf2)
            (write-file (concat file_name '.org.gpg'))
            (org-mode)
            (org-latex-export-to-pdf)
            ))
#+END_SRC
```

El código que aparece ha sido desarrollado específicamente para el actual proyecto dada la necesidad de automatizar la tarea de combinar el contenido de dos ficheros cifrados y generar un tercer fichero en formato LaTeX/PDF.
En este caso podríamos añadir argumentos como `:session s1` o `:results silent`, y obviar otros argumento como `:noweb` que no es necesario en este caso, ya que 'no' es el valor por defecto y el que especificaríamos.
Si exportamos este bloque de código tal y como está especificado, se generará el fichero `gpgFilesToPDF.el` en el directorio `.emacs.d` del usuario.
Para utilizar la función `gpgFilesToPDF` normalmente sin tener que añadirla al entorno cada vez, podemos (si el directorio `./emacs.d` del usuario está dentro del listado de la variable `load-path` de Emacs, añadir la siguiente línea al fichero `.emacs`:

```
(require 'gpgFilesToPDF)
```

Otra opción es copiar el fichero a alguno de los directorios de los que Emacs importa automáticamente los ficheros `.el`, lo que dependerá del entorno operativo y de la distribución de Emacs utilizada.
Para hacer uso de la función, primero debemos de disponer de un fichero de datos a exportar y en segundo lugar de la plantilla a rellenar y exportar.
El fichero de datos tiene el siguiente formato:

```
#+MACRO: nomProf José Luis Jerez
#+MACRO: dniProf 12345678-x
#+MACRO: cifProf A-87654321
#+MACRO: calleProf C/Eureka
#+MACRO: numProf 10
#+MACRO: localidadProf Las Rozas
#+MACRO: provinciaProf Madrid
#+MACRO: codProf 28231
#+MACRO: empCli Red Iris
#+MACRO: nomCli Francisco Moserrat
#+MACRO: dniCli 66666666-D
#+MACRO: cifCli B-99999999
#+MACRO: calleCli Plaza de Manuel Gómez Moreno, s/n - 2a planta
#+MACRO: numCli 1
#+MACRO: localidadCli Madrid
#+MACRO: provinciaCli Madrid
#+MACRO: codCli 94043
#+MACRO: telCli (+34) 91 212 76 25
#+MACRO: emailCli francsco.monserrat@rediris.es
#+MACRO: tipoServ Investigación forense
#+MACRO: codProy IF-RIRIS-POC-001
#+MACRO: costeIncumplimiento 6.000.000
#+MACRO: fechaIni Mon Mar 18 08:00:37 CET 2013
#+MACRO: fechaFin Thu Abr 18 18:00:07 CET 2013
#+MACRO: Activo_1 Fichero 'windows2003.img.gz'.
```

Donde, como se puede ver, se asigna mediante una macro, un valor (por ejemplo, `José Luis Jerez`) a una variable (por ejemplo `nomProf`).
El fichero que importa los datos y es exportado a PDF debe de tener las cabeceras que se requieran para darle el formato y propiedades deseadas y, adicionalmente, el texto a exportar, en el que se incluirán los nombres de las variables donde así se requieran, siguiendo el formato del ejemplo que aparece a continuación:

```
#+TITLE: ACUERDO DE CONFIDENCIALIDAD Y SECRETO
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:t -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)



En {{{provinciaCli}}}, a {{{date(%d-%m-%Y)}}}.

* REUNIDOS
```

```
D./Dª {{{nomCli}}}, mayor de edad, con domicilio en la C/{{{calleCli}}}
Nº {{{numCli}}}, Localidad {{{localidadCli}}}
Provincia {{{provinciaCli}}} C.P. {{{codCli}}} con
D.N.I. {{{dniCli}}}, y en representación de la compañía {{{empCli}}}, con
CIF {{{cifCli}}} y domicilio social en {{{provinciaCli}}} y,

D./Dª {{{nomProf}}}, mayor de edad, con domicilio en la C/{{{calleProf}}}
Nº {{{numProf}}}, Localidad {{{localidadProf}}}
Provincia {{{provinciaProf}}} C.P. {{{codProf}}} con
D.N.I. {{{dniProf}}}, y en representación de la compañía {{{empProf}}}, con
CIF {{{cifProf}}} y domicilio social en {{{provinciaProf}}}.

* EXPONEN

1. Que ambas partes se reconocen capacidad jurídica suficiente para
   suscribir el presente documento.

2. Que ambas partes desean iniciar una relación negocial y de colaboración
   mutua a nivel empresarial.

3. Que durante la mencionada relación las partes intercambiarán o crearán
   información que están interesadas en regular su confidencialidad y
   secreto mediante las siguientes:
```

Una vez se disponga de ambos ficheros, se abren ambos en Emacs y se ejecuta la función `gpgFilesToPDF`. En primera instancia se pedirá el nombre del buffer que contiene las distintas macros y en segunda instancia el nombre del buffer que contiene la plantilla a utilizar. Finalmente, solicita el nombre del fichero a utilizar para la exportación y realiza la misma. Dado que el fichero org generado también se cifra, Emacs solicita que se seleccione la clave de cifrado a utilizar.
Dado que hay que abrir los ficheros origen en Emacs, es indiferente si los mismos están o no cifrados. Una vez realizada la exportación se obtiene un fichero con el nombre solicitado y extensión `org.pdf`, y los correspondientes ficheros generados por TEX, que deben de ser eliminados manualmente si se cree necesario o pueden ser utilizados para realizar modificaciones manuales de los mismos desde el propio Emacs.

- Comandos y atajos de teclado básicos

  Si bien ya se han documentado los comandos básicos desde un punto de vista de investigación forense, en relación con la programación literaria, basado en las funciones `org-export-dispatch`, `command org-babel-tangle` y `org-edit-src-code` utilizamos los siguientes atajos de teclado:

  Utilizando la terminología original de Knuth, un fichero puede ser *woven* ('para humanos') o *tangle* ('para computadoras'), esto es, documentación o código.

  - `C-c-e h` exportar a HTML.
  - `C-c-e b` exportar a HTML y visualizar su contenido en un navegador.
  - `C-c-v-t` exportar los bloques de código.
  - =C-c '= abre un buffer para editar el código.

- `SHIFT-TAB` permite acceder cíclicamente a las vistas desde un nivel superior (top-level) en el que se visualizan sólo las cabeceras de primer nivel, hasta la visualización del documento completamente extendido, pasando por estados de visualización intermedios.

Capítulo 6: BUENAS PRÁCTICAS FORENSES Y DOCUMENTALES

Buenas prácticas

¿Qué son *buenas prácticas*?

En muchas ocasiones, y en diferentes foros aparecen referencias a *buenas prácticas*, *mejores prácticas* o, en inglés, *best practices*.
Si buscamos en la wikipedia, se nos indica que se entiende por *buenas prácticas* 'un conjunto coherente de acciones que han rendido buen o incluso excelente servicio en un determinado contexto y que se espera que, en contextos similares, rindan similares resultados. Éstas dependen de las épocas, de las modas y hasta de la empresa consultora o del autor que las preconiza. No es de extrañar que algunas sean incluso contradictorias entre ellas.'
En el mismo texto, comenta que en respuesta a una consulta (de la que no tengo constancia) a la Real Academia de la Lengua, esta recomienda 'el empleo de otros sintagmas alternativos, dependiendo del contexto, como mejores soluciones, mejores métodos, procedimientos más adecuados, prácticas recomendables, o similares.'
Es igualmente interesante, y no puedo estar más de acuerdo, el comentario (parcamente documentado) en la misma fuente de información, acerca de la visión crítica de las mismas, que hacen énfasis en aseverar que:

- 'la mayoría de estos términos son empleados por empresas consultoras como Accenture, McKinsey, Boston Consulting Group, Price Watherhouse, Deloitte & Touche, Stern Stewart. Ellas los comercializan y ellas mismas se encargan de convencer a las empresas para que los pongan en práctica.'
- 'Sin embargo, esos mismos detractores reconocen que no quiere decir esto que todas sean un mero producto de la comercialización de las consultoras. Aplicadas con sentido común, pueden aportar soluciones a problemas reales.'

Sin embargo, tras trabajar con distintas *mejores prácticas*, me uno al grupo que 'reconocen que las mejores prácticas son sólo un buen comienzo, mejor que una hoja en blanco, pero que no reemplazan al sentido común y a la reflexión y que, mientras se usen de manera racional y coherente, pueden acelerar la puesta en servicio de mejoras en los procesos de las organizaciones.'
Las buenas prácticas deben estar documentadas para servir de referente a otros y facilitar la mejora de sus procesos. Este es un aspecto básico de cualquier buena práctica, ya que de este modo es posible trasladar el conocimiento fácilmente a otra organización con el objetivo de aprender y mejorar.

Prácticas relevantes

Tras investigar acerca de las prácticas relevantes que hay que tener en cuenta para enfrentar un análisis forense, me he encontrado con tres elementos a tener en cuenta:

1. Prácticas legales.
2. Prácticas tecnológicas.
3. Prácticas metodológicas.

A nivel legal, cada país dispone de su propia legislación y a lo largo del PFC se hace referencia a las distintas leyes que aplican dentro del estado Español, como la Ley de Enjuiciamiento Civil (LEC) y la Ley e Enjuiciamiento Criminal (LECrim). No es objeto de este PFC adentrarse en los aspectos legales concretos, si bien se recomienda conocer la legislación o asesorarse con un abogado experto en delitos informáticos en el caso de tener que testificar como perito.

A nivel tecnológico, existe una gran cantidad de herramientas que es posible utilizar. Sin embargo, no todas son adecuadas en función , por ejemplo, de los distintos países. En USA, el uso de 'md5' para extraer y exponer un hash de un archivo o imagen forense digital en un juicio carece de valor probatorio ya que en agosto de 2004, Xiaoyun Wang, Dengguo Feng, Xuejia Lai y Hongbo Yu anunciaron el descubrimiento de colisiones de Hash para MD5. Su ataque se consumó en una hora de cálculo con un clúster IBM P690. Debido al descubrimiento de métodos sencillos para generar colisiones de hash, muchos investigadores recomiendan su sustitución por algoritmos alternativos tales como SHA-1 o RIPEMD-160. Sin embargo en España no existe tal distinción. En apartados posteriores se identificarán diferentes herramientas a utilizar durante una investigación.
En el plano metodológico internacional, se han desarrollado distintas iniciativas como directrices, buenas prácticas, y recomendaciones entre las que cabe destacar el documento ETF Request for Comments 3227 *Guidelines for Evidence Collection and Archiving* (RFC 3227), de febrero de 2002, donde se establecen una serie de principios o actuaciones básicas a considerar en la recopilación y almacenamiento de las evidencias. En algunas `fuentes de información` se comenta que en el documento se tratan aspectos relativos al análisis de evidencias, pero como se verá a continuación, esto no es correcto. Estas iniciativas permiten establecer una base de validación con el fin de probar la idoneidad del proceso ejecutado y la confiabilidad de los resultados para el juez y la parte contraría. Adicionalmente se tratan las técnicas a aplicar para obtener la evidencia digital clave para efectos de soportar las afirmaciones o declaraciones sobre una temática particular que se tenga en una diligencia civil, penal o de cualquier índole.
Quizás el documento más relevante en la actualidad es la norma ISO/IEC 27037:2012 *Guidelines for identification, collection, acquisition and preservation of digital evidence*. Este documento, que es de pago, viene a renovar el anterior documento, y de forma similar al anterior, está orientado al procedimiento de la actuación pericial en el escenario de la recogida, identificación y secuestro de la evidencia digital, sin entrar en la fase de análisis de la evidencia. Él mismo permite homogeneizar una serie de prácticas claves para efectos de dar mayor confiabilidad a los resultados de los procesos aplicados, que previamente sólo estaban fundados en la buena práctica internacional, referentes particulares a instituciones o entidades reconocidas por sus logros en este campo como veremos a continuación.
En países como Australia o USA, guías facilitadas por Standards Australia International (SAI), el National Institute of Standards and Technology (NIST) o el National Criminal Justice Reference Service (NCJRS), como:

- HB171-2003 Guidelines for the Management of IT Evidence. Australia Standard.
- NIJ (2004) Forensic Examination of Digital Evidence: A Guide for Law Enforcement.
- NIST (2007) Guidelines on cell phone forensics.
- NIJ (2008) Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.
- NIST (2010) Forensics web services.

son documentos utilizados por los investigadores forenses digitales con el fin de establecer un marco de actuación formal y verificable por terceros.
La documentación desarrollada no contempla tecnologías recientes como las unidades de estado sólido o los sistemas de control industrial (SCADA), entre otros temas especializados, que si bien pueden seguir el mismo proceso desarrollado en general para la informática forense (documentos y alcance de la norma identificación, recolección y/o adquisición, conservación y/o preservación), en muchos casos va a requerir de un enfoque particular dependiendo de su comportamiento a la hora de obtener una evidencia digital confiable. Por lo tanto, como es lógico, las distintas tipologías actuales son sensibles a cambios tecnológicos.

El reto de la informática forense pasa inexorablemente por revisiones y ajustes constantes en el tiempo de manera periódica, con el objetivo de identificar cambios y ajustes que permitan mantener la confiabilidad de los procedimientos aplicados, como quiera que este documento es un referente de alcance global.
Para terminar, comentar que los temas relacionados con el análisis e interpretación de la evidencia digital que no son cubiertos por la norma ISO/IEC 27037:2012 se espera que la anunciada ISO/IEC 27042 *Guidelines for the analysis and interpretation of digital evidence*, prevista para el 28 de febrero de 2015, sugiera los campos de acción en estos temas, los cuales tendrán retos importantes como se establece su borrador:
"El análisis e interpretación de la evidencia digital puede ser un proceso complejo. En algunas circunstancias, puede haber varios métodos que se pueden aplicar y los miembros de equipo de investigación tendrán que justificar la selección de determinado proceso y mostrar cómo es equivalente a otro utilizado por otros analistas. En otras circunstancias, los investigadores tendrán que idear nuevos métodos para el examen de la evidencia digital que previamente no ha sido tenido en cuenta y deben ser capaz de demostrar que el método de producción es 'adecuado'."

RFC 3227

El RFC 3227 presenta un línea a seguir para los procesos de recolección y archivo de evidencias digitales en casos de análisis forense digital. Este documento liberado en el año 2002, contiene recomendaciones que se han de adaptar a las tecnologías y a las circunstancias.
El índice del documento es el que se puede observar a continuación:

Table of Contents

El documento está en inglés, y se pueden encontrar traducido el español en la web para su consulta.
En el capítulo de introducción del documento, se establecen una serie de aspectos interesantes en párrafos concretos:

- 'El propósito de este documento es el de proporcionar a los administradores de sistemas las pautas para la recopilación y archivo de evidencias de dicho incidente de seguridad.'
    - Está orientado a administradores de sistemas, NO a analistas forenses.
- 'Si la recopilación de las evidencias se realiza correctamente, es mucho mas útil para la detención del atacante y existen muchas más posibilidades de que las evidencias sean admitidas en el caso de un proceso judicial.'

    - Hace hincapié en la relevancia de la corrección al tratar las evidencias de cara a un posible proceso judicial.

- 'Debería de utilizar estas pautas como base para la redacción de procedimientos de recopilación de las evidencias, y debe de incorporar estas en la documentación de los procedimientos de control de incidencias.'

    - Esta parte contradice el enfoque inicialmente comentado, la redacción de este tipo de procedimientos no debería de competer al área de sistemas.

- 'Las directrices propuestas en este documento podrían no ser adecuadas para todos los entornos o jurisdicciones. Tiene que confirmar que los procedimientos de recopilación de evidencias, una vez redactados con estas pautas, se adecuan a la ley.'

    - Estos párrafos son básicos y de extrema importancia, pese a que aparentemente no tengan una gran relevancia.

El documento plantea un proceso generalista, en el que se plantean los pasos, así como algunas de las precauciones a tomar basado en los siguientes aspectos críticos:

- **Visualizar y estudiar el escenario global** objeto de análisis. En este aspecto, es importante conocer las normas y directrices de la empresa (si existen y si respaldan las actuaciones a realizar), así como las leyes que aplican sobre la misma (privacidad).

  Debe de asegurarse que la información recopilada con las evidencias que se están buscando no está disponible al acceso de personas que normalmente no tendría acceso a dicha información. Esto incluye el acceso a los archivos de registro que podrían revelar patrones de comportamiento de los usuarios, así como archivos de datos personales.

    - No inmiscuirse en la privacidad de las personas sin una fuerte justificación para ello. En particular no tomar información de aquellas áreas en las que normalmente no existe razón alguna para acceder (por ejemplo, los almacenamientos de archivos personales), a menos que existan indicios suficientes de que existe un incidente real en los mismos.
    - Asegúrese de contar con el respaldo de la dirección de la empresa en lo relativo al establecimiento de los procedimientos para la obtención de las evidencias de un incidente.

- **Generación de la linea temporal**. Es necesario identificar todos los aspectos que permitan determinar los flujos y eventos concretos en el tiempo.

- **Recopilar las evidencias**. La evidencia debe de ser estrictamente protegida, por lo que se deben de minimizar los cambios que alteren el escenario y eliminar los agentes externos que puedan alterarlas.

    - Se deben de tomar las máximas precauciones a la hora de realizar la recopilación, con el objeto de evitar que las evidencias se borren, malogren, contaminen o modifiquen. Hay que evitar especialmente:
        - Apagar la maquina o desconectarla de la red sin haber recogido las evidencias (evaluar según sea el caso, el riesgo de intrusión o mandatos a través de sistemas y comunicaciones inalámbricos).
        - Ejecutar cualquier archivo que puedan alterar los tiempos de los ficheros.

    - Obtener una imagen lo mas exacta posible del sistema. Para ello debe de realizarse una copia a nivel de bit de los medios del sistema.
  - El procedimiento de manejo de incidentes, no deben de tener ningún tipo de ambigüedad, y debe minimizar la cantidad de toma de decisiones necesarias durante el proceso de recopilación de evidencias.
  - Desde el punto de vista de las consideraciones legales, la evidencia digital necesita ser:
    - Admisible: Se deben de haber cumplido con las normativas legales antes de ser puestas ante un tribunal de justicia.
    - Autentica: Debe ser posible vincular positivamente las evidencias con la prueba material incautada en el incidente o en la actuación.
    - Completa: Debe aportar toda la historia y no solamente una perspectiva particular.
    - Fiable: No debe existir nada referente a como la evidencia fue recopilada o manipulada con posterioridad que pudiese mostrar dudas sobre su autenticidad o veracidad.
    - Creíble: Debería ser fácilmente creíble y comprensible para un tribunal de justicia (ésta es quizás la mayor complicación).
  - Siempre que sea posible se ha de considerar la generación de checksums, utilizando una herramienta adecuada a la legislación, que firme criptográficamente la evidencia recopilada. De este modo se facilita la preservación de la Cadena de Custodia de la evidencia.

- **Priorizar la recolección de evidencias** frente al análisis de las mismas.

  - Con objeto de asegurar la validez de las evidencias recopiladas se recomienda identificar previamente y bloquear el acceso a aquellas evidencias que:
    - Revelen información personal (por vulneración de la intimidad).
    - No se ajusten a las normas legales o de seguridad de la empresa.
    - No pueda demostrarse que no ha sido manipulada.
  - Debe de evitarse realizar el análisis forense en la copia original de la evidencia. Si se desea realizar un análisis forense, para este propósito, debería realizarse una copia adicional de la evidencia a nivel de bit. Esto se debe a que, con seguridad, durante el análisis se modificarán los tiempos de registro del acceso a los ficheros.

- **Aplicar el método de recogida de datos adecuado** en cada uno de los escenarios.

  - Es precise adoptar un enfoque metódico para cada dispositivo siguiendo las pautas establecidas del procedimiento de recopilación.
  - La velocidad es, a menudo, un parámetro crítico, por lo que cuando existe un elevado número de dispositivos a examinar, es necesario distribuir el trabajo de examen entre un equipo de trabajo más amplio, para poder recoger las evidencias en paralelo. Sin embargo, cuando se trate de un único sistema, la recopilación debería hacerse paso a paso.

- **Recoger de datos ordenadamente, en función de la volatilidad de los mismos**. La *volatilidad de la información* es uno de los principales conceptos tratados en la norma, y con el objetivo de preservar dicha información, el orden propuesto para recabar la misma comprende:

  1. Registros y cache.
  2. Tablas de encaminamiento, caché ARP, tabla de procesos, estadísticas del kernel y la memoria.

3. Sistemas de archivos temporales.
4. Disco.
5. Archivos de log, registro remoto y datos de seguimiento relevante para el sistema en cuestión.
6. Configuración física, topología de red.
7. Medios de almacenamiento externos.

- **Obtener, identificar y etiquetar las evidencias unívocamente**.

  - Ser metódico.
  - Los procedimientos seguidos deben ser transparentes y reproducibles. Como cualquier aspecto de la política de respuesta a un incidente, los procedimientos deben de ser probados (por terceros independientes) para asegurar su viabilidad en una crisis. Por razones de velocidad y de precisión, los procedimientos deben de automatizarse en la medida de lo posible.

- **Mantener un registro de notas detalladas**.

  - Las notas deben incluir fechas y horas.
    - Si es posible se recomienda generar los datos automáticamente utilizando, por ejemplo, un 'script', con la prevención de asegurar que el fichero de salida generado no se ubique en los dispositivos o medios que forman parte de la evidencia.
    - Las notas e impresiones de impresora deberían estar fechadas Y firmadas.
    - Hay que tener en cuenta las diferencias existentes entre el reloj del sistema y la hora UTC (Tiempo Universal Coordinado). Para cada anotación o registro de tiempo, indicar si se utiliza la hora local o la UTC.
  - Las notas detalladas serán vitales para estar preparado para testificar,quizás años mas tarde.

- **Establecer la Cadena de Custodia desde el origen de la actuación** para el correcto mantenimiento de la integridad de la información y salvaguarda de la misma. Documentar todo lo necesario para mantener la trazabilidad del histórico y estado actual de cada una de las evidencias:

  - ¿Dónde?
    - es descubierta.
    - se recoge la evidencia.
    - es manipulada.
  - ¿Cuándo?
    - es descubierta.
    - se recoge la evidencia.
    - es manipulada.
    - se han producido cambios en la custodia de las evidencias.
  - ¿Quién?
    - descubre la evidencia.
    - recoge la evidencia.
    - ha analizado y manipulado la evidencias.
    - ha custodiado en cada momento la evidencia.
  - ¿Cómo?

        - se recoge la evidencia.
        - se han analizado y manipulado las evidencias.
        - se almacena.
        - se han producido las transferencias.
    - ¿Durante cuanto tiempo?
        - se ha custodiado la evidencia.

- **Almacenar las evidencias adecuadamente**. Las medidas a tomar para garantizar el correcto almacenamiento de las evidencias recogidas implica que éstas:

    - Deben almacenarse en un lugar seguro y a salvo de alteración, destrucción, contaminación o manipulación.
    - Debe de realizarse varias copias de la información, ya que los análisis nunca han de realizarse sobre la copia original de las evidencias.

- **Herramientas que se necesitaran**. El último apartado del documento hace referencia al echo de que se debe poseer los programas necesarios para la recopilación de las evidencias y para la actividad forense, en modalidad de sólo lectura (por ejemplo, un CD).

    - El analista forense debe estar preparado con un set de herramientas apropiadas para cada dispositivo que se prevea que va a ser necesario y que se vaya a hacer uso de él.
    - El set de herramientas debería incluir lo siguiente:
        - Programas para examinar los procesos (por ejemplo, ps).
        - Programas para examinar el estado del sistema (por ejemplo, 'showrev', 'ifconfig', 'netstart', 'arp').
        - Un programa para realizar copias bit a bit (por ejemplo, 'dd' , 'safeBack').
        - Programas para la generación de checksums y firmas (por ejemplo, 'sha 1 sum', un habilitador de checksum 'dd', 'Safeback', 'pgp').
        - Programas para la generación de imágenes del 'core' y para examinarlas (por ejemplo, 'gcore', 'gbd').
        - Programas (scrips) para automatizar la recopilación de evidencias (por ejemplo, 'FTK', 'Sleuthkit', 'Cain').
    - En el set de herramientas los programas deberían estar enlazados estáticamente y no requerir del uso de ninguna librería excepto las necesarias para los dispositivos de medios de solo lectura. Incluso así, dado que rootkits modernos pueden ser instalados a través de módulos kernel cargables, se debería considerar que las herramientas no podrían dar una imagen completa del sistema.

ISO/IEC 27037

Tal y como se ha comentado, la norma ISO/IEC 27037:2012 /Guidelines for identification, collection, acquisition and preservation of digital evidence/, viene a renovar a las ya antiguas directrices RFC 3227 vistas en el apartado anterior.
La norma está orientada a los procesos de actuación forense en el escenario de la identificación, colección, adquisición y preservación de la evidencia digital. Sin embargo, al igual que en el caso anterior, la fase de análisis de la evidencia se trata muy tangencialmente, ya que no se encuentra dentro del alcance

del documento, por lo que se espera que en la anunciada ISO/IEC 27042 *Guidelines for the analysis and interpretation of digital evidence*, prevista para el 28 de febrero de 2015, se extienda en los campos de acción relativos a estos temas.

El análisis de las evidencias es diferenciado dependiendo del tipo de dispositivo o de evidencia sobre la que se esté realizando el análisis.

Sobre este proceso de análisis la norma especifica que se ha de utilizar metodología científicamente probadas para su aplicación según las características de las evidencias y obtener la información probatoria necesaria.

El análisis ha de ser sistemático, huyendo de los exámenes intuitivos únicamente guiados y basados en la experiencia y en el conocimiento, aunque estas dos características contribuyen a la realización de un buen análisis y a llegar a las conclusiones correctas tras la interpretación de los resultados, sin embargo, sea cual sea la metodología aplicada se ha de garantizar la exhaustividad y el análisis completo y minucioso de la evidencia.

Esta norma pertenece al grupo de las normas ISO/IEC 27000 relativas a las técnicas de seguridad de la información y de las tecnologías.

El resumen que presenta la organización en su web, ya que es no un documento de libre distribución, expresa:

```
ISO/IEC 27037:2012 provides guidelines for specific activities in the
handling of digital evidence, which are identification, collection,
acquisition and preservation of potential digital evidence that can be
of evidential value.

It provides guidance to individuals with respect to common situations
encountered throughout the digital evidence handling process and assists
organizations in their disciplinary procedures and in facilitating the
exchange of potential digital evidence between jurisdictions.

ISO/IEC 27037:2012 gives guidance for the following devices and circumstances:

  - Digital storage media used in standard computers like hard
    drives, floppy disks, optical and magneto optical disks, data
    devices with similar functions,
  - Mobile phones, Personal Digital Assistants (PDAs), Personal
    Electronic Devices (PEDs), memory cards,
  - Mobile navigation systems,
  - Digital still and video cameras (including CCTV),
  - Standard computer with network connections,
  - Networks based on TCP/IP and other digital protocols, and
  - Devices with similar functions as above.

NOTE 1 The above list of devices is an indicative list and not
exhaustive.

NOTE 2 Circumstances include the above devices that exist in various
forms. For example, an automotive system may include mobile
navigation system, data storage and sensory system.
```

Como se puede extraer, habla de individuos y organizaciones, por lo que los procedimientos definidos están orientados a su uso generalizado, que se extiende tanto a los profesionales, investigadores forenses, como a componentes de las FFSSEE, por ejemplo.
El objetivo es garantizar que los procesos seguidos para el manejo de las evidencias sea correcto y que las evidencias recabadas sean válidas independientemente de su jurisdicción. Es por esto que durante el desarrollo del texto se puede apreciar que se ha evitado hacer referencia a normativas de jurisdicciones especificas. Por el contrario, y para reforzar dicho enfoque, sí se encuentran referencia a otras normas ISO 27000 para determinados aspectos referentes a la Seguridad de la Tecnología, entre ellas las ISO/IEC 27001, la ISO/IEC 27002, así como la ISO 17020 y la ISO/IEC 17025, por lo que el contenido es de uso y aplicación universal.
Finalizando el análisis del resumen, podemos ver que las tipologías de dispositivos y entornos tratados en la norma son, entre otros:

- Equipos y medios de almacenamiento y dispositivos periféricos.
- Sistemas críticos (alta exigencia de disponibilidad).
- Ordenadores y dispositivos conectados en red.
- Dispositivos móviles.
- Sistema de circuito cerrado de televisión digital (CCTV)).

A continuación se presenta el índice completo de la norma, y se puede observar la evolución que ha experimentado frente al RFC 3227 [1]:

[1] He añadido el índice completo ya que me parece interesante poder observar la evolución de la norma frente al RFC 3227, y por otro lado, he sido autorizado por escrito por AENOR (tras consultar con ISO copyright office), tal y se puede verificar en el documento anexo ISO_IEC_27037_2012.pdf.

Dado que, como se ha comentado, la norma no es de libre distribución[fn:6_2:

attribute the portions to “Mapping the Forensic Standard ISO/IEC 27037”(2013).] como en el caso del RFC 3227, en los siguientes subapartados trataré de forma resumida, y sin citar textos concretos, los aspectos más relevantes, en mi opinión, que desarrolla la misma. Dado que la norma es bastante densa en contenidos, me he centrado en los aspectos más operativos, y en lo que respecta a la evolución de este texto frente a su antecesor.

Acrónimos

Si bien el vocabulario utilizado no varía frente al resto de documentación, he identificado dos acrónimos que son interesantes, relacionados con algunos de los individuos o equipos responsables de la identificación, recolección, adquisición y preservación de las potenciales evidencias digitales, y que nombraré en distintos momentos:

DEFRs Digital Evidence First Responders.

DESs Digital Evidence Specialists.

Requisitos para la correcta gestión de evidencias digitales

Los requisitos sobre los procesos que expresa la norma para el manejo de las evidencias digitales son:

- **General**: En la medida de lo posible, la evidencia digital debe ser adquirida del modo menos intrusivo, preservando la originalidad de la prueba y realizar posteriormente las copias de respaldo necesarias.
- **Auditable**: Los procesos deben establecer las medidas necesarias para disponer de las evidencias y trazas de todas las acciones realizadas y de sus resultados. Al igual que en el RFC, los procedimientos deben haber sido validados por terceras partes, de forma que se asegure que siguen buenas practicas profesionales.
- **Repetible**: Los procedimientos deben de ser repetibles y para ello, las herramientas utilizadas deben de ser documentadas previa validación por parte de terceros del uso para el cual se utilizan en la actuación.
- **Reproducible**: Los procedimientos utilizados deben de ser reproducibles por terceros en cualquier momento, manteniendo el resultado inicial documentado.
- **Justificable**: Los procedimientos y las evidencias deben de ser comprensibles para los entendidos en la materia, quienes puedan dar validez y respaldo a las actuaciones realizadas.

Cadena de Custodia

El concepto de *Cadena de Custodia* no varía. Se basa en el uso de un documento que recoja todos los aspectos relativos a la gestión de las evidencias digitales.
La trazabilidad de la gestión de las evidencias digitales es el objetivo de mantener una Cadena de Custodia férrea. De esta forma es posible identificar aspectos como quien tuvo acceso a los dispositivos digitales o datos en cualquier punto dado en el tiempo.
La Cadena de Custodia de las evidencias es uno de los aspectos clave en un proceso judicial, y ésta debe ser mantenida durante todo el proceso, ya que un error en la misma puede derivar en la anulación de la evidencia asociada a dicha Cadena de Custodia.
Como se ha comentado en distintas ocasiones, la Cadena de Custodia debe de ser establecida desde el momento inicial en que el dispositivo digital y los datos digitales se han obtenido y no debe ser rota a lo largo del tiempo.

La Cadena de Custodia debe contener información que permita identificar al DEFR, un identificador único para el componente custodiado, fecha, hora y lugar de la identificación y recogida, así como los datos relativos a las sucesivas custodias posteriores de la misma y las diferentes ubicaciones donde se desplace.

Documentación, documentación, documentación

La documentación es un aspecto fundamental a tener en cuenta para la correcta gestión de un proyecto de análisis forense digital.
La Cadena de Custodia es parte de la documentación, una parte crítica de la misma, pero no es la única documentación a desarrollar.
El momento en el que se desarrolla un análisis forense y el momento en el que el mismo es evaluado por las autoridades competentes puede ser muy distante en el tiempo. Es por ello que el detalle de las notas tomadas durante todo el proceso puede ser crítico a la hora de plantear detalles de las acciones realizadas frente a un tribunal, sobretodo si han pasado años desde el suceso.
Cada uno de los procesos que se desarrollen debe de documentarse adecuadamente, ya que durante las fases iniciales se realizan muchas actividades que, si no son documentadas, pueden caer en el olvido y complicar o malograr un trabajo de análisis profesional. Cualquier omisión de información puede, posteriormente, pueden ser crítica a la hora de plantear el trabajo frente a un tribunal.
Si bien se trata de una obviedad, es sumamente importante tomar nota de los identificadores únicos de los dispositivos tales como número de serie así como cualquier traslado de los dispositivos.
Finalmente, al igual que se comentó anteriormente, debe de prestarse especial atención a la configuración horaria de los distintos dispositivos digitales que están conectados y son sensibles a la hora y fecha. Es necesario, y debe de formar parte explícita del proceso, verificar el valor de tiempo reflejado en los distintos dispositivos con una zona horaria común y documentar cualquier aspecto relevante, como dispositivos con distinto uso horario o con configuraciones manuales que no se adecúan al uso común establecido.

Prioridad en la actuación: Orden de volatilidad

Los dispositivos que pueden contener evidencias digitales pueden ser tantos y tan variados que es absurdo tratar de listarlos. Los más evidentes son ordenadores, teléfonos, smartphones, etc pero cualquier elemento susceptible de contener datos digitales se puede considerar un dispositivo a adquirir.
Previo a la recogida de los distintos dispositivos es necesario realizar una identificación de los mismos, dando prioridad a aquellos que puedan contener datos volátiles ya que éstos pueden ser fácilmente destruidos o perdidos para siempre si no se conserva la *diligencia debida* o due diligence para protegerlos. Por ello, antes de apagar ningún dispositivo, debe de analizarse la idoneidad de tal acción y documentar previamente el estado del mismo sin alterarlo. Posteriormente se tratará este aspecto en diferentes ámbitos.
El personal que manipula los distintos dispositivos debe poseer el conocimiento necesario para priorizar las labores de recolección de acuerdo a la volatilidad de los datos de los dispositivos.
Este tipo de medidas carece de sentido en los dispositivos con datos residentes, ya que los mismos se mantienen en los medios de almacenamiento incluso si la fuente de alimentación es apagada o eliminada.

Ámbito de actuación

Como he comentado, el ámbito de actuación en el que nos movemos es muy amplio. Sin embargo hay una serie de elementos que, en caso de estar presentes en el escenario, son críticos a la par que evidentes, como son los ordenadores personales (fijos o portátiles), dispositivos de almacenamiento, dispositivos

móviles, sistemas de circuito cerrado de televisión digital (CCTV) y, si los anteriores se encuentran interconectados a dispositivos de red (electrónica de red, en general) se amplía el campo de búsqueda en función del criterio del analista forense a servicios externos que pueden estar vinculados con la investigación. Otros elementos menos obvios son dispositivos como impresoras, contestadores automáticos y, en general, dispositivos que asociamos en menor medida a la gestión de datos, pero que también son objeto de la investigación.
En esencia, y como veremos a continuación, muchos de los tratamientos de los distintos dispositivos son idénticos o muy similares.
Y, llegados a este punto,¿se puede complicar más el escenario? Pues sí.
En la actualidad 'la nube' ya es un elemento común a tener en cuenta dentro de los escenarios diarios del entorno digital. En la práctica es una extensión del escenario anterior en el que el Centro de Datos (CPD) se podía ver envuelto dentro del ámbito de la actuación. Pero 'la nube' incorpora una variable de 'deslocalización' que es importante tratar adecuadamente.
No es objeto de este PFC tratar la casuística particular en la que 'la nube' es parte del ámbito de actuación. Sin embargo, dado que me parece un tema interesante y que, a corto plazo, se va a convertir en un elemento crítico en las actualizaciones forenses, he investigado acerca del acercamiento de los profesionales a este tipo de proyectos.

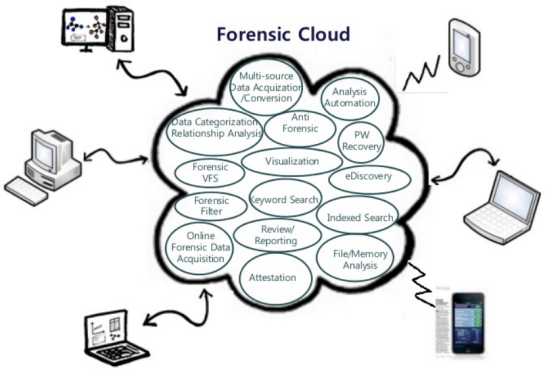


Figura 1: `http://www.slideshare.net/00heights/the-future-of-digital-forensics`

Me ha parecido particularmente interesante el planteamiento presentado durante la conferencia de la RSA 2013 por Sung-kyong Un, acerca de la evolución y el futuro del análisis forense digital, así como el documento Mapping the Forensic Standard ISO/IEC 27037 to Cloud Computing[fn:6_3: © 2013 Cloud Security Alliance – All rights reserved.
You may download, store, display on your computer, view, print, and link to "Mapping the Forensic Standard ISO/IEC 27037" at `https://cloudsecurityalliance.org/research/imf/` , subject to the following:(a) the Document may be used solely for your personal, informational, non-commercial use; (b) the Document may not be modified or altered in any way; (c) the Document may not be red istributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the paper as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to "Mapping the Forensic Standard ISO/IEC 27037"(2013).], editado por la Cloud Security Alliance en junio de 2013, y que plantea como acometer un 'cloud forensics' frente a un 'forense tradicional' dentro de un escenario global en el que combina la ISO/IEC 27035:2011 con los estándares:

- ISO/IEC 27035:2011 Information security incident management
- ISO/IEC DIS 27041 Guidance on assuring suitability and adequacy of incident investigative methods
- ISO/IEC DIS 27042 Guidelines for the analysis and interpretation of digital evidenceq

- ISO/IEC DIS 27043 Incident investigation principles and processes

Con el objetivo de cerrar el círculo de todo el ámbito de investigación de un incidente.

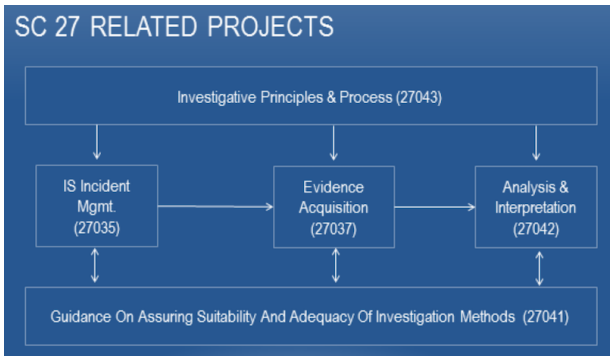


Figura 2: Cloud Security Alliance

Procesos en los que se divide la actuación

Para cada tipología de dispositivo, la norma divide la actuación o su tratamiento en tres procesos diferenciados como modelo genérico de tratamiento de las evidencias:

Identificación proceso que implica la búsqueda, reconocimiento y documentación de las potenciales evidencias digitales ya sean físicas o lógicas (virtual). No se trata de una tarea sencilla, ya que la localización real de los datos puede ser compleja en grandes sistemas de almacenamiento con configuraciones tolerantes a fallos, por ejemplo.

Recolección y adquisición Tras el proceso de identificación de potenciales evidencias digitales, éstas deben de ser recolectadas o adquiridas.

- La recolección es el proceso de recopilación de elementos que contienen las pruebas digitales potencial. Es más o menos equivalente a la práctica estándar de aplicación de la ley de incautación de elementos que contienen la potencial evidencia digital bajo la autoridad de una orden jurídica (es decir, una orden de registro) y llevarlos a un laboratorio forense u otro centro para su preservación, procesamiento y posterior análisis.
- La adquisición es el proceso de creación de una copia de los datos dentro de un sistema definido. Se trata de la práctica más común en el sector privado debido a la necesidad de reducir al mínimo el impacto en el negocio durante una investigación en curso. Para este proceso en particular, dada la variedad de posibles métodos de adquisición (imagen de disco, copia de datos a distintos destinos, etc) es muy importante aplicar los aspectos comentados en el apartado `Requerimientos para la correcta gestión de evidencias digitales`, esto es, que el proceso sea comprensible, defendible y bien documentado. Además, es importante que el proceso incluya medidas que garanticen la integridad de las copias durante su adquisición.

Preservación Una vez la evidencia digital ha sido recolectada o adquirida, ésta debe de ser preservada con el objetivo de garantizar su integridad y su utilidad, es decir, su originalidad para que posteriormente ésta pueda ser admisible como elemento de prueba original e integra en un proceso judicial. Este proceso es tan importante como complejo dada la fragilidad de las evidencias digitales.

Buenas prácticas durante el proceso de identificación

Para la correcta identificación de todas las potenciales evidencias digitales se debe de aislar, inicialmente, cada uno de los componentes del escenario a analizar de sus *capacidades de interconexión*, esto es, de los interfaces que le permiten comunicar con diferentes entornos tecnológicos como IEEE 802.3, 802.11, 802.15.
Un ordenador es una potencial evidencia en si mismo, independientemente de si está conectado a una red, ya sea mediante un cable físico o conexión inalámbrica, o de los dispositivos periféricos electrónicos conectados al mismo que reciben (impresoras), procesan (dispositivo móvil) o almacenan datos (pen drive).
Así mismo, cada uno de dichos elementos, como soportes de almacenamiento (discos duros, memorias flash, CDs, DVDs, disquetes, cintas magnéticas o pen drives), impresoras, escáneres, cámaras web, reproductores de MP3, sistemas GPS o dispositivos RFID entre otros, son potenciales evidencias digitales a ser tratadas.
La existencia de equipos o dispositivos en red implica que el escenario es ampliable en función del criterio del analista forense a la hora de acotar dónde se encuentran los datos. En ese punto, es necesario identificar equipos vinculados al escenario como servidores, otros ordenadores de distintos usuarios localizados geográficamente en distintos puntos, puntos de acceso a la red, dispositivos bluetooth, y electrónica de red en general (hubs, switches, routers) etc.
Las buenas prácticas más relevantes, desde mi punto de vista, a tener en cuenta por parte del DEFR durante el proceso de identificación son:

- Seguir estrictamente la legislación, normativas y procedimientos que pudieran afectar a la gestión de las evidencias digitales.
- Asegurar la escena del incidente de modo que ninguna persona no autorizada puede tener acceso a los dispositivos que pueden contener evidencia digital.
    - Entre otros aspectos, hay que minimizar el riesgo de que una persona, dado el reducido tamaño de muchos dispositivos de datos o de los móviles, pueda sustraer o dañar algún de los que se encuentran en el escenario inicial.
- Registrar el escenario del incidente mediante el uso de fotografías, esquemas o filmación y reflejar la escena tal como se encuentra al inicio, siempre de acuerdo con las circunstancias de costes y de tiempo. Es posible que, basado en el criterio del analista forense, el escenario a registrar se extienda al CPD u a otras localizaciones.
    - Si el ordenador está encendido, se ha de fotografiar la pantalla y documentar la hora y fecha del reloj frente al actual, así como el estado del indicador de duración de la batería (en el caso de equipos portátiles) o hacer un escrito descriptivo con lo que aparece en la misma.
    - Si el dispositivo móvil está encendido, grabar y tomar fotografías de cualquier símbolo o indicadores en la pantalla como el icono del teleoperador, los SMS, llamadas perdidas, hora/fecha del reloj frente al actual (de referencia) y el indicador de duración de la batería.
    - Prestar especial atención a la hora de identificar, sobre el escenario, los tipos de dispositivos que pueden ser relevantes para el caso.
- Garantizar que los dispositivos de comunicación no estén en situación de recibir o transmitir datos.
    - Debe de usarse una caja de Faraday o una caja blindada para impedir que el dispositivo obtenga conexión a la red ya que la conexión a una red GPRS, 3G/4G, inalámbrica, o similar puede dar lugar al deterioro de posibles pruebas digitales, debido a posibles llamadas y mensajes entrantes.

- Identificar y documentar (tipo, marca, modelo, número de serie, localización, etc) todos los posibles elementos de prueba o contenedores de las mismas (ordenadores, los dispositivos periféricos, etc) para su posterior recolección o adquisición.

- Mantener invariable el estado de los equipos (encendido o apagado) y dispositivos periféricos, en la medida de lo posible.

    - Identificar los posibles medios de carga (cargadores, cunas) y el cables de los dispositivos que tienen baterías y que pueden funcionar sin conexión, para asegurar que la información no se pierde. Éstos serán recopilados o adquiridos junto con el dispositivo que posee la evidencia digital durante el proceso pertinente.
    - Los dispositivos que estén funcionando se deben mantener conectados a la red eléctrica para asegurar que la información no se pierde.
    - Se recomienda la entrega inmediata de los dispositivos móviles encendidos al laboratorio para su análisis.
    - Si el dispositivo móvil esta apagado:
        - Se analizan las acciones de empaquetado, precintado y etiquetado del dispositivo.
        - Hay que evitar cualquier funcionamiento accidental a deliberado de las teclas a botones.
        - Es aconsejable el usa de una caja de Faraday o cajas blindadas.

- El DEFR debe tener especial cuidado para no contaminar posibles evidencias no digitales (huellas dactilares, el ADN y las partículas) y coordinarse con los recolectores de pruebas que sean pertinentes con el fin de asegurar dichas pruebas antes de proceder con siguientes pasos.

- Utilizar un dispositivo que permita identificar, localizar y monitorizar señales inalámbricas los dispositivos inalámbricos conectados.

Buenas prácticas durante el proceso de recolección o adquisición

Una vez finalizado el proceso de identificación, el DEFR debe decidir entre recolectar los dispositivos o adquirir las evidencias digitales directamente de los mismos.
La elección tiene que estar en equilibrio con las capacidades del DEFR (disponer de una orden legal adecuada) y las circunstancias relativas al coste, tiempo y recursos disponibles.
En cualquier escenario, el DEFR necesita realizar una imagen de los medios de almacenamiento de los dispositivos susceptibles de contener evidencias digitales.
El DEFR debe decidir entre recolectar los dispositivos o adquirir las evidencias digitales 'in situ' directamente de los mismos.
La norma establece que pueden darse tres escenarios distintos en los que hay que plantearse el proceso adecuado de recolección o adquisición, y para cada una de las situaciones la norma establece unas secuencias de pasos a seguir para preservar la evidencia contenida en los dispositivos. Los escenarios son:
1.- Los equipos están encendidos.
2.- Los equipos están apagados.
3.- Los equipos están encendidos pero no pueden ser apagado.
Sin entrar en detalles concretos, se establecen las siguientes directrices para la recolección o la adquisición de dispositivos:

- El orden de recogida viene en función de la volatilidad de los datos.

- Decidir, en función de la naturaleza del caso, del dispositivo y de los recursos disponibles, que dispositivos se van a recopilar para su análisis posterior y en cuales se van a llevar a cabo las actuaciones en el lugar de la adquisición.
    - Los dispositivos recolectados deben ser colocados en embalajes adecuados para la naturaleza de los dispositivos incautados, de modo que los mismos, o los datos que contiene, no sean dañados.
- Verificar que se dispone de los datos (marca, modelo y numero de serie) de cada uno de los dispositivos gestionados.
- Etiquetar adecuadamente todos los elementos de prueba.
    - Todo dispositivo se debe sellar con precintos, ser etiquetado y firmarse en la etiqueta.
    - Las etiquetas de las pruebas no deben ser colocadas directamente en las partes mecánicas de los dispositivos electrónicos, ni debe cubrir o esconder información importante.
    - Se debe etiquetar las pruebas con tinta en lugar de lápiz ya que el polvo del grafito del lápiz puede interferir con la lectura del disco o cinta.
- Los dispositivos recogidos se deben de preservar en un ambiente de clima seguro y controlado que no este sujeto a temperaturas extremas o a humedad.
- En el caso de los dispositivos con conectividad a algún tipo de red hay que tener en cuenta que no hay que modificar el estado de las comunicaciones hasta que se ha asegurado que no hay pérdida de evidencias como resultado de la desconexión. Entonces se puede retirar los dispositivos de la red.
- Para las redes de cableado de datos, trazar (realizar un croquis) de las conexiones con los equipos y etiquetar los puertos para la futura reconstrucción de la toda la red.
- En el caso de los dispositivos móviles, hay que tener en cuenta que:
    - Si el dispositivo está encendido, existen distintos servicios (como Bluetooth, RF, pantalla táctil, IR) pueden estar activados o desactivados.
    - Algunos deben estar encendidos para acceder al modulo y extraer la información, mientras que otras adquisiciones de información se puede realizar directamente desde la tarjeta SIM.
    - Los diferentes fabricantes utilizan diferentes sistemas operativos que requieren diferentes métodos de adquisición de datos.
    - Para dos imágenes del mismo dispositivo, se muestran diferentes valores de hash. Esto es debido a las actualizaciones internas del sistema como puede ser, por ejemplo, la diferencia entre la hora en que se hizo cada una de las copias.
- Realizar el tratamiento de cada equipo, siendo tratado como un equipo independiente.

Buenas prácticas durante el proceso de preservación

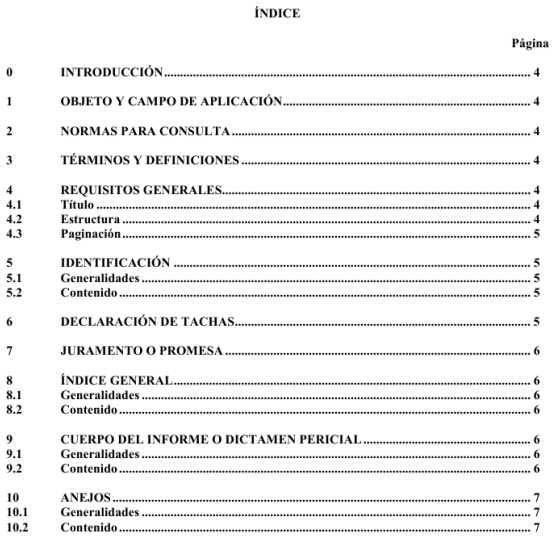
Todos los dispositivos recolectados y potenciales evidencias digitales adquiridas deben ser preservadas frente a perdida, daños o deterioros potenciales.
El objetivo más importante en el proceso de preservación es mantener la integridad de la Cadena de Custodia de dispositivos y datos digitales.
Para preservar las posibles evidencias digitales:

- Una de las garantías que debe ofrecer el analista forense a las partes y al juez, es la verificación de la identidad o correspondencia entre los elementos de prueba originales y sus duplicados, a través de la obtención de valores matemáticos de comprobación conocidos como "Hash", que son valores numéricos, resultado de la suma de números tomados de los datos objeto del señalado proceso. El Hash o valor de comprobación debe ser idéntico entre las posibles evidencias originales y los copiados.
- Los dispositivos recolectados deben mantenerse envueltos en envases adecuados para la naturaleza de los mismos con el fin de evitar la contaminación de los dispositivos digitales durante los transportes a otro lugar. En particular:
    - Los discos duros deben ser preservados mediante balsas antiestáticas.
    - Las CPUs y los portátiles deben ser preservados mediante un contenedor apropiado para evitar daños o deterioro de las evidencias digitales que contienen.
- Todos los dispositivos digitales:
    - Deben de mantenerse precintados utilizando medidas a prueba de posibles manipulaciones y mantener la Cadena de Custodia.
    - No deben ser expuestos a campos magnéticos, polvo, vibraciones, humedad o a cualquier otro elemento del medio ambiente que pueda dañarlos.
    - Deben mantenerse almacenados en un ambiente controlado donde no estén sometidos a temperaturas o humedad extremas.
- Los dispositivos, en particular los móviles, pueden tener la capacidad para borrar los datos y por lo que cualquier interacción manual con el dispositivo debe ser minimizada.

UNE 197001:2011

El informe forense es el elemento que consolida los diferentes procesos que dan soporte a un análisis forense digital.
En general, las diferentes fuentes que he consultado[2] coinciden en que el informe debe de estar basado en una metodología científica con las adaptaciones a los distintos sistemas implicados y a las actividades criminalísticas analizadas, que el ámbito de la investigación requiera.
Tras investigar y buscar información acerca de metodologías utilizadas para el desarrollo de informes forenses digitales o estándares que conduzca a aportar formalidad y calidad en los informes, me ha sorprendido no encontrar documentación estandarizada en países como USA, Australia, y otros en los que, por el contrario, he identificado que el resto de procesos sí están evolucionados y documentados.
La norma UNE 197001:2011 'Criterios generales para la elaboración de informes y dictámenes periciales', fue publicada por AENOR (Agencia Española de Normalización y Certificación) el 23 de Marzo de 2011.
La norma tiene por objeto establecer los apartados que se consideran mínimos necesarios a incluir en la elaboración de un informe, sin ser éstos una enumeración excluyente, limitativa ni exhaustiva; así como precisar los requisitos formales que deben tener los informes, sin determinar los métodos y procesos específicos para la elaboración de los mismos. En resumen, podríamos decir que son las normas necesarias para desarrollar el documento final que refleja nuestra investigación.
En la siguiente imagen aparece el índice de la norma[3], que como se puede apreciar, no es significativamente extenso para lo que se podría pensar.

[2] La documentación referida son los libros que aparecen en la bibliografía aportada en el proyecto.
[3] Se ha solicitado permiso expreso a AENOR para la publicación del índice de la norma UNE 197001:2011.



ÍNDICE

Página

Figura 3: Indice de la norma UNE 197001:2011

La norma, si bien a nivel de contenidos está muy poco desarrollada y su alcance es general en lo que corresponde al ámbito de informes periciales, permite establecer una estructura común para todos los análisis forenses digitales y agrega un valor diferenciador para aquellos profesionales cualificados que se preocupan por mejorar cada día en la complicada tarea de ser analista forense.
Se recomienda, para evidenciar que se están siguiendo estándares y buenas prácticas para la redacción del informe, redactar explícitamente un texto en el que se exponga que dicho informe se ha desarrollado siguiendo la normativa UNE 197001:2011.
Además, se recomienda leer la norma, ya que su extensión, como se ha dicho, no implica un gran esfuerzo. A modo de resumen de los distintos apartados, se puede extraer como contenidos más relevantes:

- REQUISITOS GENERALES

  La norma marca que un informe forense debe de contener los siguientes elementos básicos:

  - Título: Elemento que debe de identificar al documento de forma inequívoca, acorde al contenido del texto del informe.
    - Debe ser explicativo en relación a la temática del informe.
    - No deben de nombrarse evidencias o actores.
    - Asociar el código de referencia, ya que éste es único.
  - Documento: Se compone de varios apartados claramente diferenciados que se desarrollarán a continuación (identificación, declaraciones, índice, cuerpo del informe y anexos).
  - Paginación: Todas las páginas deben estar numeradas.

- IDENTIFICACIÓN

  Respecto de la identificación que debe de aparecer en todas las páginas del documento, ya sea en la cabecera o el pie del mismo, se define expresamente que:

  - Debe contener todos los datos necesarios para identificar el informe.
  - Debe incluir:
    - Título.

- Código de referencia (único).
  1. Es responsabilidad del analista forense establecer un mecanismo de nombrado único para asignarlo a sus informes.
  2. Un mismo código no puede ser asociado a dos informes distintos.
  3. A modo de recomendación, el código puede formarse uniendo mediante guiones (FIM-MAL-01-01):
     a) Siglas identificativas del peticionario (3 caracteres).
     b) Siglas identificativas del tipo de informe (3 caracteres).
     c) Código de versión (2 dígitos).
     d) Código de revisión (2 dígitos).
- Datos del peticionario de la actuación.
- Datos del destinatario del informe.
- Código de expediente o procedimiento (si lo hubiera).
- Identificación del perito (nombre y apellidos, DNI, asociación pericial a la que pertenece).
- Identificador del letrado o procurador (si procede)).
- Fecha de liberación del informe.
- Datos de la localización física del análisis.
  1. Dirección.
  2. Coordenadas GPS o UTM.
  3. Enlace a Google Maps.

- DECLARACIÓN DE TACHAS

  El analista forense debe de expresar por escrito que actúa de buena fe y que no existe ningún motivo por el cual deba de abstenerse de realizar el informe.

- JURAMENTO O PROMESA

  El informe pericial no puede ser desarrollado por una persona relacionada con el proceso. El analista debe de ser independiente y objetivo, además de poseer los conocimientos necesarios para desarrollarlo.

  Este texto es en cierto modo irrelevante, ya que el mero hecho de aceptar el trabajo de realizar el informe conlleva las obligaciones que desarrolla ésta declaración. La misma implica que el analista forense:

  - Está procediendo bajo juramento o promesa de decir la verdad, y haber actuado con la mayor objetividad e imparcialidad posible.
  - Está en conocimiento de las sanciones penales de no actuar de ese modo.

- ÍNDICE GENERAL

  En el presente apartado se explica que su objetivo es facilitar la búsqueda y localización de la información por los diferentes capítulos.

  Se debe de incluir el esquema básico del informe, que se compone de los títulos y numeración de los puntos más relevantes del informe llegando a la profundidad que el analista forense considere, siempre que se respeten las normas de simplicidad y claridad.

- CUERPO DEL INFORME O DICTAMEN PERICIAL

  El cuerpo del informe:

  - Es el elemento integrador de las partes que componen el proceso global de análisis forense. Integra:
    - Los procesos y buenas prácticas seguidas.
    - Las evidencias identificadas.
    - Las investigaciones y el razonamiento analítico aplicado.
    - Las conclusiones objetivas extraídas.
  - Debe de tener una extensión suficiente, sin excederse debido a explicaciones superfluas o ser incompleto por no haber facilitado la suficiente información.
  - Debe de ser comprensible para el juez, abogados y otros profanos en la materia, evitando tecnicismos.
  - El idioma utilizado debe de ser el castellano, si bien se permite expresarse y redactar el informe en la lengua oficial de la Comunidad Autónoma.
  - Debe de ser correcto, léxica, sintáctica y semánticamente.

  Los puntos a desarrollar son:

  - Objeto. Aclara la finalidad del informe forense, e introducir qué es lo que se pretende con todo el trabajo realizado.
  - Alcance. Tal como indica su título, en este apartado se desarrolla el alcance de cada una de las cuestiones que se plantaron en el apartado anterior de forma que quede claro para el receptor del informe que se ha cumplido con los objetivos acordados, y, en caso de que el alcance se haya modificado durante el desarrollo del proyecto (siempre de mutuo acuerdo), que todo aparezca claramente reflejado. Además, se desarrollarán aspectos como los procesos, recursos, limitaciones, esfuerzo y presupuesto.

- Antecedentes. Son los hechos acontecidos con anterioridad al inicio del análisis forense y que sirven de punto de partida del mismo.

Sin embargo, los antecedentes no deben de condicionar el resultado del informe, y deben de tomarse como una fuente más de información que debe de ser tratada.

- Consideraciones preliminares. Dado que el informe se desarrolla a posteriori, al redactar este apartado conocemos lo que pensábamos, como analistas previo a realizar el análisis y la certeza o errores de nuestras consideraciones previas. Aquí se desarrolla todo lo que el analista forense considere necesario para explicar las decisiones tomadas en función de la información que se tenía en ese momento, como se desarrolló el trabajo, qué bases teóricas dieron lugar a la utilización de una u otra tecnología, los procedimientos seguidos, así como las limitaciones y restricciones que existieron en cada momento.

Toda esta información permitirá conocer y entender como se ha realizado el trabajo, porque se ha identificado y extraído determinadas evidencias y otras se han podido perder, y cómo se ha llegado a las conclusiones presentadas.

- Documentos de referencia. Libros, documentos, manuales, normas, información obtenida de URLs, etc. Cualquier soporte, físico o electrónico, que haya sido utilizado para desarrollar el análisis forense.

- Terminología y abreviaturas. Todos los términos tecnológicos y abreviaturas que se han usado en la redacción del informe.
- Actuaciones. Cada acción que ejecuta el analista forense debe de estar justificada previo a realizarla, y documentada durante todo el proceso, de modo que el analista forense se encuentre en disposición de contestar cualquier cuestión que se le plantee posteriormente.

Este apartado es especialmente importante el las actuaciones complejas, ya que la memoria no es fiable.

- Análisis. Toda la labor realizada por el analista debe de quedar, de la forma más explícita y resumida posible, plasmada y justificada en este apartado.

Debe de aparecer reflejado todo el proceso, fundamentado en buenas prácticas o experiencias previas a falta de las primeras, todas la situaciones que se han ido dando, la resolución de las mismas y cualquier explicación que permita comprender, sin lugar a dudas, el porque de cada paso dado y su necesidad.
Para toda aquella información que sea demasiado extensa o técnica se tendrá que evaluar la necesidad o idoneidad de que aparezca en este apartado o en los anexos, haciendo referencia a los mismos.

- Conclusiones. Sólo deben de desarrollarse las conclusiones de las cuestiones planteadas. Ésas deben de ser:
  - Objetivas.
  - Precisas.
  - Claras.
  - Justificadas.
- ANEJOS. No existen normas predefinidas para éste apartado. Cualquier aspecto que, por la razón que sea, no haya podido ser desarrollado a lo largo del informe se puede y debe de añadir en como anexo y deben de formar parte del mismo como cualquier otro punto, e incluirlos en el índice.
  - Cualquier documento, nota, fotografía que ayude a entender o reforzar el contenido de la pericial.
  - Temas técnicos tratados en profundidad.
  - Descripción de los méritos, menciones, titulaciones y certificaciones, experiencia y trayectoria que acreditan al analista forense como experto en la materia sobre la que se ha realizado el informe.
  - Datos relativos a la fecha de solicitud del informe, el plazo dado para la realización del mismo y cualquier evento que haya podido modificar en el tiempo los resultados del análisis, como retrasos justificados o injustificados.

Hay muchos profesionales que piensan que sólo los informes forenses que cumplan con el contenido de este estándar deberían de ser admitidos como entregables para un proceso penal ya que permite identificar las capacidades del analista forense o, por lo menos, que sigue las normas marcadas para la realización del análisis forense.

Capítulo 7: METODOLOGÍA PROPUESTA

Metodología de investigación digital forense basada en Emacs

> 'El artículo 18 del Estatuto de los Trabajadores autoriza la realización de registros sobre la persona del trabajador, en sus taquillas y efectos particulares, pero sólo en determinadas circunstancias (cuando sea necesaria para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa), y con determinadas condiciones (dentro del centro de trabajo y en horas de trabajo; respetando al máximo la dignidad e intimidad del trabajador y contándose con la presencia de algún representante legal de los trabajadores).'[1]

Por otro lado:

> Noviembre, 2000. Sala de lo Social en Málaga. Tribunal Superior de Justicia de Andalucía.
>
> La sentencia resultado del juicio realizado a raíz de la denuncia efectuada por un trabajador contra el empresario que accedió a su equipo de trabajo, y copió todos sus correos y ficheros personales en presencia del comité de empresa se inclina en este apartado por el criterio empresarial, a pesar de que la sentencia en cuestión da la razón al trabajador, pero sólo por el hecho de que no se justificó el registro tal y como obliga el artículo 18 del Estatuto de los Trabajadores.
>
> La resolución afirma implícitamente, que el mencionado artículo 18 autoriza el registro en la terminal de ordenador que utiliza el trabajador. A todos los efectos, un equipo se asimila a la taquilla, basándose en que el ordenador es un instrumento de trabajo propiedad de la empresa. Por lo tanto, no deberá ser utilizado con otros fines diferentes que la realización de la propia actividad laboral.

Con esta introducción no pretendo ahondar en cuestiones tales como si los archivos personales y el correo electrónico de los trabajadores son simples 'efectos particulares', o pertenecen al ámbito de la intimidad del trabajador, ya que no son objeto de este PFC [2]. Sin embargo, quería destacar la importancia de conocer y acatar la legislación vigente, al margen de las buenas prácticas a aplicar.
Una vez finalizadas las explicaciones acerca de las buenas prácticas estandarizadas, voy a combinar en la medida de lo posible dicho conocimiento con algunos de los conocimientos que he recabado de lecturas de libros, blogs y documentación varia que se recoge en la bibliografía, y así disponer de una metodología propia acorde con las buenas prácticas y experiencias de terceros, incluyendo las mías propias.
En mi opinión, el hecho de que el origen de determinada información no sea parte de la documentación de un estándar no le quita valor, ya que se trata del conocimiento de los expertos que trabajan día a día en este campo, y que, en resumen, aplican el sentido común a una labor ya de por si 'desquiciante' en muchos casos.
Una buena práctica que se repite mucho es, que si el equipo está encendido, es una buena opción obtener una fotografía de la pantalla y apagarlo. ¿Y esta práctica no va en contra de los estándares anteriormente comentados? Pues no. Puesto que pudiera haber información importante relativa a archivos temporales o archivos críticos como, en el caso de sistemas Windows, el de paginación de memoria, podría optarse por apagar el equipo cortando el suministro de energía. Obviamente, en este procedimiento, la pérdida más relevante la constituyen la información relativa a la red y a la memoria RAM. Sin embargo, tal como comenta la norma y el estándar, hay que tener presente las circunstancias del caso y el tipo de escenario al que hay que enfrentarse para adoptar la decisión adecuada. En el caso de que la información de red y de la memoria RAM fuesen críticas, sería imprescindible contar con testigos que pudieran refrendar las

[1] `http://archivo.cnt.es/Documentos/legislacion/legi_correoe.htm`.

[2] Un artículo interesante al respecto 'PROBLEMAS DERIVADOS DE LA UTILIZACIÓN DEL CORREO ELECTRÓNICO E INTERNET EN EL ÁMBITO LABORAL' es accesible en `http://www.uria.com/documentos/publicaciones/1235/documento/trib04.pdf?id=2029`.

acciones realizadas y que pudieran atestiguar que no se ha realizado ninguna acción enfocada a manipular datos, sólo a adquirirlos. No obstante, siempre habrá que tener prevista una respuesta en la vista judicial para una defensa de las acciones realizadas.

Muchas organizaciones integran en sus procedimientos mecanismos para hacer uso de testigos en casos concretos, como intervenciones de equipos de trabajo en procesos complejos. Para estos casos, suele requerirse que todo el proceso de identificación, recolección o adquisición de las posibles evidencias digitales sea llevado a cabo en presencia de una persona del comité sindical y el propio afectado, o en su defecto dos personas de la organización totalmente independientes a las circunstancias del caso. La integración de dichos mecanismos en los procedimientos derivados de los procesos forenses garantiza, sobretodo si hay que entrar en procesos judiciales, la correcta ejecución de los procedimientos, habiéndose realizado una serie de acciones específicas, con testigos concretos que pueden refrendar los hechos.

Al inicio del proyecto o investigación, antes de iniciar ningún proceso, hay que dar respuestas (por escrito) a una serie de preguntas fundamentales. Algunas de las preguntas básicas son:

1. LEGISLACIÓN y NORMATIVA: ¿Cuál es la legislación y normativas a aplicar?

2. ALCANCE: ¿Cuál es el escenario ante el que hay que enfrentarse?

3. ÁMBITO: ¿Qué quiere analizarse: un fichero, un directorio, un disco o todo un sistema?

4. POSIBLES IMPLICADOS: ¿Se trata de un incidente ejecutado por personal externo o puede haber personal interno implicado?

5. ANTECEDENTES: ¿Existe algún antecedente similar? ¿Se ha alterado el escenario en algún modo?

6. LIMITACIONES: ¿De cuánto tiempo se dispone para hacer la adquisición de las evidencias?

7. NECESIDADES DE PRESERVACIÓN: ¿Dónde y cómo se almacenarán las evidencias?

8. TIPO DE ANÁLISIS: ¿Cuántas copias deben realizarse?

He observado que en ocasiones los profesionales e incluso los mismo estándares, tratan en distintos procesos las mismas actuaciones (procedimientos). Un ejemplo claro es el procedimiento de copia de disco, que se trata en la adquisición y el análisis, por lo que, con el objetivo de tratar de simplificar y clarificar la metodología propuesta, he aplicado el sentido común a la hora de desarrollar cada uno de los procesos, tratando de no repetir actuaciones iguales en procesos distintos. Sin embargo, y dado que hay actividades muy relevantes, estas aparecerán reiteradas para mayor concienciación del lector.

A continuación, tal como he comentado, he recogido las prácticas de distintos profesionales a la hora de trabajar sobre el terreno y, de acuerdo al contenido de los estándares de investigación forense y buenas prácticas actuales, tanto técnicas como normativas o legislativas, he desarrollado una propuesta que abarca desde el inicio de una investigación digital forense hasta la consolidación de la misma en forma de informe forense, que igualmente, está alineado con los estándares de documentación internacionales.

Procesos básicos de una investigación forense

En general, está consensuado que existen cinco procesos básicos que se suceden de forma continua y con dependencia de precedencia entre los mismos, de modo tal, que hasta que un proceso no finaliza, no comienza el siguiente. Los cinco procesos son:

1. Preparación.
2. Identificación.
3. Recopilación o adquisición.
4. Preservación.
5. Análisis.
6. Consolidación.

Cada uno de estos procesos tiene que estar basado en la Ciencia y en la Técnica y adecuadamente documentado, seguir una metodología estructurada adecuada a la actuación, ser sistemático, de forma que sus fases permitan que el proceso sea completo y exhaustivo. Además, los procesos tienen que ser capaces de ser reproducibles y comprensibles por un experto en la materia, así como proporcionar las trazas necesarias para contrastar las acciones realizadas y los resultados obtenidos.
Es importante reiterar que los procesos, dependiendo del ámbito y alcance sobre el cual se esté realizando la actuación, siempre deben de estar basados en protocolos conocidos de actuación y en buenas practicas como las vistas en apartados anteriores.
Para abarcar por completo el alcance de una investigación forense, en algún proceso, se han especificado algunas acciones que no se pueden realizar directamente con Emacs por completo, por ejemplo la realización de fotografías o las entrevistas con el personal involucrado, sin embargo, en algún punto de la metodología estas acciones se alinearán con el uso de Emacs, ya se incluyendo las fotografías como parte del informe forense (desarrollado en Emacs) o redactando las actas de las entrevistas.
Por otro lado, si bien se ha tratado la metodología como una secuencia de procesos, la realidad es que prácticamente en la totalidad de las investigaciones es muy complicado esperar a que finalice cada una de las fases para iniciar la siguiente, por lo que muchas veces la investigación implica mantener en paralelo varios de los procesos al tratar distintos activos o evidencias. Sin embargo, el orden de los procesos `siempre` debe de respetarse. No es posible iniciar la adquisición de una evidencia sin que esta haya sido adecuadamente identificada o sin disponer de la documentación necesaria que autoriza al investigador a acceder al escenario de la investigación.
En el caso del proceso final de consolidación, en el PFC se hará referencia a la misma desde el punto de vista del informe, en el que se `presentan por escrito` los resultados de la investigación. Queda fuera del alcance el planteamiento de la presentación de los resultados en un juicio.
Como se verá a continuación, durante el desarrollo de los procesos que componen la metodología propuesta se van ha nombrar y describir elementos de información que son necesarios para el correcto desarrollo de la investigación. Como parte del desarrollo de cada uno de los procesos de la metodología propuesta se facilita una descripción y la correspondiente plantilla (en caso de que sea necesaria para complementar la descripción) de cada uno de los documentos que se proponen.
Cada uno de estos elementos conforma, en parte o en su totalidad, un documento concreto que debe de ser creado, mantenido y finalizado adecuadamente, en función de la metodología propuesta, por el investigador. La extensión de los documentos es variable, y el hecho de que alguno de ellos pueda ser concreto y escueto no es razón para obviarlo o tratar de integrarlo en otro fichero forzando una relación que no aporte consistencia a la documentación global.

En la metodología planteada, la integridad y cifrado de documentos desde el momento inicial forma parte de la misma, por lo que en el momento de la creación de cada uno de los documentos, su extensión será '.org.gpg'. De esta forma aseguramos que la información no pueda ser accedida[3], y por lo tanto manipulada, sin las credenciales adecuadas.
Obviamente, los ficheros cifrados no van a ser los entregables finales, sino que sus contenidos serán exportados a formato PDF para su entrega al receptor de los mismos.
Los procesos críticos que componen la metodología de investigación forense digital basada en Emacs son:

Proceso de preparación

Todo el mundo conoce la frase *¿Preparados?... ¿listos?... ¡Ya!*, que es el pistoletazo de salida de muchos eventos.
De nuevo la semántica es un aspecto interesante en tanto en cuanto las dos cuestiones iniciales que plantea la frase, en el contexto de arrancar un evento se refiere al estado 'hasta el momento' y 'en el momento' de los participantes.
La correcta preparación de una investigación permite prevenir errores en procesos posteriores o malos entendidos derivados de la falta de concreción documental que suele convivir con todo tipo de proyectos.
Durante la preparación del proyecto no se accede a ningún activo del cliente.
El objetivo del proceso de preparación es disponer de toda la documentación necesaria para el correcto inicio de la investigación, por lo que se han identificado los siguientes documentos con el fin de cumplir con dicho objetivo:

- Registro de acciones realizadas (RAR)

  Nunca es una buena idea el dejar a la memoria la responsabilidad de recordar todas las acciones realizadas durante la investigación, ni siquiera establecer una tarea diaria que obligue al investigador ha realizar un listado de las tareas realizadas y documentar el estado.

  Cada vez que se inicia una tarea, por insignificante que sea, debe de ser documentada mínimamente. No se trata de incrementar el trabajo del investigador con una tarea que impacte sensiblemente en el tiempo estimado para el desarrollo de la investigación, pero es necesario que el proceso sea transparente y repetible.

  Al utilizar Emacs como procesador de textos, que permite trabajar con buffers sin necesidad de crear un fichero concreto, es posible desarrollar el registro de acciones desde el momento inicial, incluso antes de crear los directorios, que sería el paso siguiente, y disponer de datos pormenorizados desde el primer momento.

  El documento debe de contener los datos relativos al profesional que realiza la acción, además de la acción como tal, los tiempos empleados, la identificación de la evidencia si se trabaja sobre alguna o varias de ellas y los resultados obtenidos.

  En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de registro de acciones realizadas que puede servir como ejemplo para este tipo de documentos. Adicionalmente, a continuación se presenta una posible plantilla que se ha desarrollado y adaptado para su uso mediante Emacs tal y como se puede ver en el siguiente enlace.

- Plan de proyecto (PP)

[3] En Configuración se especifica que el fichero de configuración no debe de generar ficheros temporales. Éstos podrían dar lugar a una posible fuga de información.

La planificación de proyectos forma parte de la gestión de proyectos, la cual se vale de cronogramas tales como diagramas de Gantt o TaskJuggler 3 para su gestión, si bien es posible utilizar otro software como MS Project, para planear el progreso dentro del entorno de la investigación.

La finalidad de la planificación de un proyecto es crear un plan de proyecto que un responsable de proyectos pueda usar para gestionar el progreso del equipo de investigadores. Adicionalmente, es el proceso que permite cuantificar el tiempo y recursos que un proyecto requiere.

Dado que Emacs está vinculado con la herramienta Taskjuggler, ésta es una potente opción a la hora de planificar.

Se han desarrollado para el proyecto varios ficheros de ejemplo que se encuentran en el directorio 'PFC - PLANIFICACIÓN'. Están basados en el desarrollo del presente PFC, pero no se trata de ficheros completos.

Si bien es posible utilizar un solo fichero para la planificación y seguimiento de un proyecto, creo más adecuado estructurarlo en varios ficheros. A continuación se presenta el fichero de configuración principal de Taskjuggler (.tjp), y los ficheros que incluyen la especificación de actividades (.tji) que desarrollé inicialmente para el desarrollo del PFC, y que posteriormente utilicé como plantilla para desarrollar la planificación de la prueba de concepto realizada.

- `./PLANIFICACION/00-Planificacion_PFC.tjp`: Fichero principal que especifica los aspectos más generalistas del proyecto como horarios, festividades, especificación de informes, y otros aspectos globales, y que en general, puede ser reutilizado sin apenas cambios para investigaciones futuras.
- `./PLANIFICACION/10-proyecto_FC.tji`: Fichero que es incluido en el principal y que especifica las distintas tareas, dedicación y particularidades de la investigación a planificar. Para diferenciar explícitamente los tiempos planificados de los tiempos realmente empleados se utilizarán dos escenarios distintos:

  plan escenario planificado.

  actual escenario real.
- `./PLANIFICACION/20-jljerez.tji`: Si bien la dedicación puede ser especificada en el fichero anterior con un formato que consolida la totalidad de la misma en el parámetro `complete` indicando el tanto por ciento de avance de la tarea, este parámetro es una simple referencia. La forma concreta de indicar la dedicación de cada recurso es mediante la especificación de los espacios de tiempo dedicados a cada una de las tareas o actividades descritas, lo que es conocido como `booking`. Este formato de reporte de dedicación está directamente relacionado con la gestión del tiempo que propone la presente metodología, ya que como puede verse a continuación, la notación en ambos casos es muy similar en concepto. El reporte de horas en Taskjuggler se presenta como:

```
actual:booking pfc.ini.planProy 2015-05-27-15:31-+0100 + 6.32h,
                                2015-05-27-07:35-+0100 + 6.40h,
```

y en el caso de Emacs, el detalle del tiempo dedicado a una tarea se especifica como puede verse a continuación

```
** Plan de proyecto
  CLOCK: [2015-05-27 Wed 15:31]--[2015-05-27 Wed 22:03] =>  6:32
  CLOCK: [2015-05-27 Wed 07:35]--[2015-05-27 Wed 14:15] =>  6:40
```

En el capítulo dedicado a la prueba de concepto se desarrolla un plan de proyecto que puede servir como ejemplo para este tipo de documentos:

- Fichero principal de la PoC.
- Fichero de especificación de tareas y planificación inicial.
- Fichero de dedicación del recurso (booking).

Y el resultado obtenido se puede ver en el siguiente enlace.

- Estructura de directorios de trabajo

  Previo al inicio de un proyecto forense se recomienda disponer de un directorio de trabajo desplegado sobre una partición cifrada, ya sea local[4] o remota[5]. Éste es un aspecto crítico, ya que toda la información de proyecto debe de estar protegida desde el inicio del proyecto hasta el final.

  Adicionalmente, se deben de aplicar los medios y permisos adecuados con el fin de restringir el acceso a la documentación sólo al personal autorizado.

  En el caso de que se utilicen contraseñas, ya sea de forma personal o para compartirlas en equipo, éstas deben de estar siempre protegidas[6] y no deben de facilitarse a personal no autorizado.

  Finalmente, se debe de disponer de una estructura de directorios predeterminada en la que almacenar la documentación desarrollada así como las evidencias identificadas con sus correspondientes documentos de cadena de custodia.

  Disponer de una estructura común para todos los proyectos asegura una ordenación común de los ficheros creados, lo que permitirá al perito mejorar el tiempo de acceso a los mismos a lo largo del proyecto y posteriormente,

  Para ello, a continuación se facilita una alternativa para disponer de un entorno de proyecto adecuado en sistemas Linux, Mac y Windows.

  La estructura de directorios de trabajo propuesta, independientemente del sistema operativo que se utilice por parte del investigador, es:

```
\PROYECTOS
   \codProy
      \PreProyecto
      \Planificación
      \Evidencias
      \Informe
```

  Esta estructura de directorios es muy básica, y puede y debe de ser modificada por el investigador en la medida que lo estime oportuno.

  En sistemas Linux y MacOS, previo a la creación de la estructura de directorios base del proyecto tal como se especifica anteriormente, se va a crear un sistema de ficheros cifrado utilizando encfs. Tras la instalación del sistema de ficheros se podría utilizar Emacs para automatizar, por ejemplo, las siguientes tareas:

[4] Se propone TrueCrypt como herramienta de cifrado local, si bien también es posible utilizarla como herramienta de cifrado remoto.a

[5] Se propone encfs como herramienta de cifrado remoto.

[6] Se propone keepass como herramienta de gestión de contraseñas, si bien se podrían utilizar pass para entornos Linux/Mac o simples ficheros de texto cifrados con gnupg.

```
Creación del entorno de trabajo

 #+begin_src sh :eval never :results silent :exports none
   cd {{{dirProy}}}
   mkdir {{{codProy}}}
   mkdir {{{codProy}}}.cod
   encfs {{{dirProy}}}/{{{codProy}}}.cod {{{dirProy}}}/{{{codProy}}}
   cd {{{dirProy}}}/{{{codProy}}}
   mkdir PreProyecto
   mkdir Planificacion
   mkdir Evidencias
   mkdir Informe
 #+end_src

Montar el entorno de trabajo

  #+begin_src sh :eval never :results silent :exports none
encfs {{{dirProy}}}/{{{codProy}}}.cod {{{dirProy}}}/{{{codProy}}}
  #+end_src

Desmontar el entorno de trabajo

   #+begin_src sh :eval never :results silent :exports none
 fusermount -u {{{dirProy}}}/{{{codProy}}}
   #+end_src
```

En el caso de sistemas Microsoft Windows se puede utilizar encfs4win, pero también es posible utilizar aplicaciones como TrueCrypt para montar un directorio/unidad de disco cifrado, que permita disponer de un directorio de trabajo desplegado sobre una partición cifrada.

- Acuerdo de confidencialidad (AC)

  Cualquier profesional de la seguridad debe ser consciente de la importancia que tiene la información que se maneja.

  La protección del cliente es una de las bases de la filosofía de un buen servicio de seguridad.

  El acuerdo de confidencialidad (también llamado, contrato de confidencialidad) es un acuerdo cuyo objetivo principal es el de preservar el secreto o la confidencialidad de la información.

  Es recomendable, por tanto, firmar un acuerdo de confidencialidad que nos comprometa como profesionales a no difundir la información a la que se tenga acceso mientras se desarrolla la investigación.

  Se ha desarrollado una plantilla de acuerdo de confidencialidad utilizando documentación de la web de Inteco (Acuerdo de confidencialidad) y se ha adaptado para su uso mediante Emacs tal y como se puede ver en el siguiente enlace.

- Antecedentes (ATC)

  En el documento de antecedentes se debe de especificar la razón concreta por la que el cliente contacta con el investigador forense para proponerle el proyecto, y el contexto previo a la llegada del investigador.

En el citado documento debe de comentarse aspectos como por ejemplo, si ha existido algún antecedente similar, y en caso de que se haya alterado el escenario, en algún modo se han dado dichas alteraciones.

En particular, no debe de aparecer ningún tipo de nota especulativa acerca de los comentarios del cliente. El investigador debe de mantener siempre la objetividad en cualquier circunstancia.

En el caso de los antecedentes no se ha considerado necesario la elaboración de una plantilla debido a su escasa complejidad. Se trata básicamente de un acta de reunión en el que se deben de documentar los aspectos citados y cualquier antecedente adicional.

En el capítulo dedicado a la prueba de concepto se desarrolla un documento de antecedentes que puede servir como ejemplo para este tipo de documentos.

- Datos generales de la investigación (DGI)

  El fichero de datos generales se compone de los datos que van a ser utilizados para, en combinación con las distintas plantillas y utilizando la función Emacs Lisp gpgFilesToPDF generada para el actual PFC, generar automáticamente y de forma segura varios documentos finales.

  En el caso del fichero de datos generales se ha elaboración una plantilla. Se trata básicamente de un fichero que especifica una línea de MACRO por cada uno de los conceptos a los que se referencia desde las diferentes plantillas se pueden ver en el siguiente enlace.

  Además, en el capítulo dedicado a la prueba de concepto se desarrolla un documento de datos generales que puede servir como ejemplo para este tipo de documentos.

- Aceptación y autorización de trabajos (AAT)

  En ningún caso debe de iniciarse una investigación sin disponer de un documento de aceptación y autorización de la misma. En el caso de que no se dispusiera del mismo y se diese algún tipo de problema legal, el investigador está expuesto a responsabilidades que podrían derivar en penas incluso de privación de libertad, independientemente de que el responsable real pudiese ser el propio cliente.

  El documento debe de especificar aspectos tales como los que se enumeran a continuación, o los datos relevantes que se considere necesario concretar previo al inicio de la investigación:

  1. ALCANCE: ¿Cuál es el escenario ante el que hay que enfrentarse?
  2. ÁMBITO: ¿Qué quiere analizarse: un fichero, un directorio, un disco o todo un sistema?
  3. NECESIDADES DE PRESERVACIÓN: ¿Dónde y cómo se almacenarán las evidencias?
  4. TIPO DE ANÁLISIS: ¿Cuántas copias deben realizarse?

  Se ha desarrollado una plantilla de autorizacion y aceptacion de trabajos adaptada para su uso mediante Emacs tal y como se puede ver en ./PLANTILLAS/Autorizacion y aceptacion de trabajos.org

- Registro de limitaciones y exclusiones (RLE)

  Previo al inicio de la investigación debe de delimitarse y especificarse por escrito el ámbito de acción de los investigadores. Las principales razones son dos:

  LIMITACIONES Acotar adecuadamente las expectativas del cliente.

  LEGISLACIÓN y NORMATIVA Prever posibles problemas legales en caso de acceder a ámbitos que quedan fuera del alcance de la investigación.

Derivado de las razones enumeradas, como parte de la documentación del proyecto, se desarrollará un documento en el que se especifiquen aspectos tales como los sistemas a los que NO se va a acceder, el tipo de pruebas que NO se van a realizar, datos que NO se van a investigar, así como, en caso de ser relevante y necesario, limitaciones derivadas del tiempo que se dispone para hacer la adquisición de las evidencias o el análisis de las mismas.

Adicionalmente, derivado de la revisión del contexto legal que afecta al escenario, dispositivo, elemento o información que se va a analizar, se especificarán las autorizaciones legales necesarias, cuales son los prerrequisitos de la investigación, sobre qué se debe actuar, quién debe intervenir, quién puede estar presente y cual es el limite legal de la actuación. Por ello es necesario conocer perfectamente la legislación y normativas a aplicar en cada caso.

En el caso del registro de limitaciones y exclusiones se ha elaboración una plantilla de ejemplo. Se trata básicamente de un documento en el que se deben de documentar los aspectos citados y cualquier limitación adicional.

`./PLANTILLAS/Registrodelimitacionesyexclusiones.org`

Adicionalmente, en el capítulo dedicado a la prueba de concepto se desarrolla un documento de limitaciones y exclusiones que puede servir como ejemplo para este tipo de documentos.

- Documento de inicio de proyecto (DIP)

  El documento de inicio de proyecto desarrolla las líneas maestras del proyecto y debe de ser firmado por el cliente previo al inicio de la investigación.

  El objetivo del documento es contextualizar el proyecto y especificar los parámetros más relevantes del mismo. Este documento debe de ser el origen de las respuestas ante cualquier duda o problema con el cliente acerca del desarrollo de la investigación.

  En el documento, además de los parámetros de categorización del proyecto, se deben especificar los datos del cliente, la planificación prevista y la firma de aceptación del cliente.

  Se ha desarrollado una plantilla que adaptada para su uso mediante Emacs tal y como se puede ver en siguiendo el enlace a ./PLANTILLAS/Documento de inicio de proyecto.org

  Es recomendable en este caso, que a la hora de utilizar la plantilla, se realice una copia de la misma antes de empezar a modificarla ya que algunos campos utilizados importan datos del documento de datos generales y otros campos a cumplimentar deben de ser desarrollados explícitamente sobre el documento, por lo que se modificaría la plantilla original.

  Se puede ver un ejemplo del mismo desarrollado durante la prueba de concepto en

Proceso de identificación

Si una investigación se traduce en un fracaso la causa de ello, en términos generales, normalmente radica en la investigación inadecuada que se ha practicado en el escenario de los hechos.
Se podría decir que, el éxito o fracaso de la investigación, dependerá de cómo se actué en el proceso de identificación. Para ello se debe de tener muy claro el alcance y objetivo del proceso, que no es otro que `determinar, registrar y describir` cada una de los activos que componen el escenario objeto de la investigación, independientemente de si finalmente son considerados evidencias en si mismos, contenedores de evidencias o don descartados para tal fin.
Un ejemplo claro de los activos involucrados a identificar son los equipos informáticos, sin entrar en el detalle de identificar cada una de los dispositivos de almacenamiento que pueda tener conectados salvo que el acceso sea inmediato al mismo y no implique ningún tipo de modificación del estado del activo principal. Por lo que se podrá identificar cualquier dispositivo USB conectado al equipo pero no el disco duro interno del mismo, y mucho menos ficheros concretos del sistema.

En el proceso de identificación hay aspectos relevantes a considerar previo a su desarrollo en función de si el origen y objetivo de la actuación es por:

Orden judicial Si se requiere, es posible la recolección (incautación) de evidencias para su posterior análisis en el laboratorio. Se tiene que contar con:

- La presencia de un secretario judicial.
- Un requerimiento de la actuación que se precisa por parte del perito.

Solicitud de un particular, empresa, institución, u otra parte Será responsabilidad del solicitante facilitar información que permita al investigador forense establecer que el solicitante está en posesión de los derechos legítimos sobre la que tiene que actuar y, por tanto, existe la posibilidad e idoneidad de llevar a cavo la recolección de evidencias. Se tiene que contar con:

- La presencia de un notario.
- Un encargo por escrito y firmado por el solicitante, en el que se describa claramente el alcance de la investigación (equivalente al documento de autorización y aceptación de trabajos, de la fase de preparación), y que autorice al investigador forense para la realización de la actuación.

En cualquier investigación es importante conocer los *antecedentes* (obtenidos en la fase de preparación) del caso, para permitir conocer la situación actual, realizar un posicionamiento frente al modo de afrontar la investigación y tomar la decisión tratando de determinar el proceso que se desea seguir para crear la estrategia a poner en practica en la búsqueda de la información y las evidencias necesarias.
Por ello, tras disponer de los aspectos relevantes iniciales así como de los antecedentes, y previo a la identificación efectiva de las posibles evidencias, se han de considerar aspectos tales como:

- Revisión del contexto legal que afecta al escenario, dispositivo, elemento o información que se va a analizar, las autorizaciones legales necesarias, cuales son los prerrequisitos, sobre que se debe actuar, quien debe intervenir, quien puede estar presente, cual es el limite de la actuación. La actuación debe transcurrir dentro de los parámetros de la legalidad, de tal modo que una incidencia no invalide las posibles evidencias obtenidas.

- Revisar que, para realizar una actuación correcta y adecuada sobre el objeto de la investigación, se dispone de:

  - Los conocimientos técnicos necesarios: conocimientos técnicos, legales, normativos.
  - Los procedimientos adecuados: tanto la *metodología* como los *procedimientos concretos* incluidos en la misma y utilizados durante la investigación deben de estar por escrito previo al inicio de la misma.
  - Las herramientas hardware y software necesarias: *checklist de herramientas y de artefactos*.

- Dado que, como se ha visto, en este punto de la investigación es imposible diferenciar entre un activo involucrado en la investigación y las distintas evidencias concretas que puede contener el mismo, ya que éste puede ser una evidencia en si mismo, es necesario:

  - Identificar la totalidad de los elementos informáticos (o activos del escenario) y documentarlos adecuadamente en un *documento de identificación de activos* (referido como 'Formulario de registro de evidencias' en algunos textos) de forma que se disponga de toda la información necesaria acerca del estado de la información (almacenada, en procesamiento o en desplazamiento) a recabar como posibles evidencias.

- Etiquetar (y obviamente documentar) adecuadamente los activos/evidencias con los detalles suficientes como para obtener una identificación unívoca.

  Se debe de imposibilitar que alguien modifique datos sobre una evidencia.
- Obtener información (sin alterar los mismos en forma alguna) que permita identificar cada uno de estos dispositivos, y añadir una descripción con cualquier aspecto significativo que se haya observado.
- Anexar fotografías o filmaciones como parte de la documentación del formulario (de las pantallas encendidas, discos, equipos electrónicos, y en general cualquier elemento identificado como evidencia).

A modo de guía, y tras las consideraciones anteriormente desarrolladas, el investigador está en disposición de iniciar la identificación efectiva de las posibles evidencias en el escenario a analizar.
Si bien no se va a actuar sobre los activos ya que las tareas se limitan a la identificación de los mismos, algunas de las precauciones que debe tomar el investigador, así como los pasos a seguir son:

- Actuar estrictamente dentro del alcance definido en la orden o en el encargo recibido. Se debe de obtener la autorización adecuada para proceder a actuar (y documentarlo en el *registro de incidencias*):

  - En caso de dudas acerca del alcance.
  - Sobre elementos que se encuentren fuera del alcance definido.

- Registrar las credenciales de los actores participantes y su vinculación con la actuación en si misma mediante la *documentación de identificación de actores y cuadro relacional*.

- Previamente al acercamiento físico al escenario (si es el caso) y a los distintos dispositivos, debemos de disponer de las medidas adecuadas para no crear falsos rastros o indicios. Se recomienda el uso de `guantes de látex` (sí, eso pone, además de la investigación digital debe de tenerse en cuenta la investigación forense clásica) para la colocación de las etiquetas.

- Reconocer el escenario:

  - Etiquetar con etiquetas de activos/evidencias numeradas unívocamente todos los dispositivos físicos que componen la escena y material que va a ser secuestrado.

- Fotografiar y filmar el entorno globalmente.

  - Dispositivos informáticos, entrando en el nivel de detalle necesario y suficiente en lo referente a elementos identificativos (etiquetas, serigrafías o similar).
  - Documentación impresa, agendas, diagramas, planos, libros o similar.

- Anotar aquello que pueda ser singular o anormal en el *registro de incidencias*.

- Confeccionar con exactitud y fidelidad los diversos *croquis del escenario* integrando todos los elementos, tanto electrónicos como arquitectónicos, que puedan ser relevantes para la investigación (la decisión queda del lado del investigador). El croquis o plano viene a constituir el esqueleto y la fotografía el músculo que permite conformar el retrato de la escena objeto de la investigación.

En este punto, hay quien hace referencia a aspectos de la recolección o adquisición de datos, como la toma de decisiones en el caso de identificar dispositivos encendidos. Sin embargo, por higiene mental y coherencia metodológica, todos esos aspectos son tratados en los siguientes apartados.

Figura 1: Etiquetas

- Registro de incidencias (RI)

  Durante cualquier investigación se suceden incidentes no previstos que pueden afectar al desarrollo del proyecto en mayor o menor medida. Se trata de situaciones como la imposibilidad de acceder a un sistema en un momento dado, reuniones planificadas que no tienen lugar o son retrasadas, denegación de accesos a dispositivos o similar.

  Es importante registrar todas las incidencias y la evolución de las mismas con el objetivo de evitar situaciones de conflicto en algún momento. El investigador es responsable de llevar a cavo la investigación, sin embargo, no puede ni debe tomar decisiones que no le corresponden.

  En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de registro de incidencias que puede servir como ejemplo para este tipo de documentos. Adicionalmente, a continuación se presenta una posible plantilla que se ha desarrollado y adaptado para su uso mediante Emacs tal y como se puede ver a continuación:

  `./PLANTILLAS/Registrodeincidencias.org`

- Identificación de elementos o palabras clave (IEP)

  Uno de los grandes problemas a la hora de realizar una investigación es tener claro lo que se está buscando. Es realmente complicado conocer a ciencia cierta los hechos e iniciar la investigación con una línea clara desde el primer momento.

  Dado que normalmente lo que al investigador se le va a facilitar es con una serie de elementos tales como usuarios, sistemas, intervalos horarios o palabras clave con un significado más o menos conocido, es necesario que esos datos se encuentren recogidos en un documento concreto.

En el caso de los elementos o palabras clave no se ha considerado necesario la elaboración de una plantilla debido a su escasa complejidad. Se trata básicamente de una lista en la que se deben de documentar los aspectos citados y cualquier dato adicional que pueda estar relacionado.

En el capítulo dedicado a la prueba de concepto se desarrolla un documento de elementos o palabras clave que puede servir como ejemplo para este tipo de documentos.

- Identificación de actores (IA) y cuadro relacional (CR)

  ¿Se trata de un incidente ejecutado desde el exterior por personal externo o puede haber personal interno implicado? ¿Qué relación se establece entre los distintos actores identificados?

  Las preguntas planteadas, entre otras, son las que responde el documento de actores en conjunto con el cuadro relacional.

  El objetivo es disponer de un documento que proporciona información similar a las aplicaciones de minería y recolección de información que se utilizada durante la fase de `Data Gathering`, proceso que forma parte de los proyectos de hacking ético, en el cual se trata de obtener el mayor número de información posible sobre un objetivo para su posterior ataque. En este caso, el objetivo es el contrario, dado que se trata de obtener el mayor volumen de información sobre los posibles participantes en un ataque.

  En el caso de la documentación relativa a actores y cuadro relacional no se ha considerado necesario la elaboración de una plantilla debido a su complejidad y el nivel de personalización que puede desarrollarse. Se trata básicamente de un listado en el que se debe de visualizar los actores, sus relaciones y, en la medida de lo posible, su involucración en relación a la cronología de los hechos conocida en cada momento.

  En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de documentación de la identificación de actores y cuadro relacional que puede servir como ejemplo para este tipo de documentos.

- Identificación de activos involucrados (AI)

  ¿Activos?... ¿Evidencias?... Son en el fondo elementos objeto de identificación para su posterior análisis.

  Los activos involucrados son evidencias en potencia.

  Cada elemento informático relacionado con el incidente a investigar puede ser en si mismo una evidencia, o contener internamente una o varias evidencias relacionadas con el objeto de la investigación.

  Es necesario disponer de un documento que permita identificar, siguiendo las buenas prácticas que se describen en la metodología, cada uno de los activos involucrados, por lo que se recomienda disponer de un documento concreto o formulario a tal efecto. Sería el equivalente a un inventario de activos/evidencias que disponga de toda la información de las mismas, incluyendo fotos donde se vean las etiquetas asociadas en el caso de evidencias físicas, o los metadatos en el caso de evidencias digitales.

  En el caso de la documentación relativa a la identificación de activos/evidencias se trata básicamente de un listado en el que se debe de visualizar los activos, sus identificadores, documentos gráficos (fotografías o vídeos), fecha y hora de su identificación, sus relaciones y cualquier observación de interés al respecto, como puede observarse en la plantilla de ejemplo que se ha desarrollado:

  ./PLANTILLAS/Registro de activos.org

  Sin embargo, la plantilla de registro de activos, debido a su complejidad y el nivel de personalización que puede desarrollar cada investigador, y a las particularidades de la investigación, debe de ser modificada y ampliada por el mismo en función de sus necesidades.

En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de documentación de la identificación de actores que puede servir como ejemplo para este tipo de documentos.

- Croquis del escenario global (CEG)

  Integrando todos los elementos relativos a actores, línea temporal, elementos, palabras clave, evidencias y cualquier elemento que aporte información que permita ser esquematizada se obtiene el croquis del escenario global.

  En el caso del croquis del escenario global no se ha considerado necesario la elaboración de una plantilla debido a su complejidad y el nivel de personalización que puede desarrollarse. Se trata básicamente de un croquis que relaciona los datos mencionados anteriormente mediante algún tipo de grafo.

  Existen varias aplicaciones que, mediante el desarrollo de ficheros de datos utilizando texto plano con tecnologías como javascript, XML o similar, permiten especificar elementos, propiedades de los mismos y relaciones entre ellos, por lo que Emacs es un entorno óptimo para su utilización.

  Derivado del nivel de integración con Emacs planteamos la herramienta ditaa como una buena alternativa, si bien es posible utilizar otras la facilidad de uso de esta herramienta la convierte en nuestra primera elección.

  En el capítulo dedicado a la prueba de concepto no se desarrolla un ejemplo de croquis del escenario global dada la escasa complejidad del mismo. Sin embargo, sí se explica en el capítulo 8 un planteamiento que puede servir como ejemplo para este tipo de documentos.

Proceso de recolección o adquisición

Hasta llegar al punto actual de la investigación, el 100 % de las acciones realizadas han sido pasivas, esto implica, que en ningún momento se ha alterado el escenario objeto de la investigación.
La fase de preparación proporciona la documentación necesaria, relativa a las autorizaciones que se requieren para acceder al escenario objeto de investigación y continuar con el proceso metodológico forense.
Una vez finalizado el proceso de identificación inicial y en función de los activos identificados, el siguiente paso es la recopilación de los mismos.
En este punto se inicia la documentación relativa a la *Cadena de Custodia*, la cual, a partir de que da comienzo la actuación no puede ser rota ya que de otra forma invalidaría su capacidad probatoria.
Es muy importante recalcar, de nuevo, la necesidad de disponer por escrito y conocer la metodología necesaria para garantizar la integridad de la Cadena de Custodia para cada elemento y situación considerada.
El proceso de recolección (incautación) sólo puede ser ejecutado por personal con las credenciales adecuadas y los conocimientos que les permitan identificar, en función del tipo de dispositivo, tipo de información y el entorno del cual se debe extraer la información que conforma la evidencia, el método óptimo para preservar la misma.
En caso de recolectar algún dispositivo, éste debe de ser precintado y salvaguardado adecuadamente.
El proceso de adquisición es una labor que debe ser ejecutada por un profesional experto para garantizar la correcta manipulación y metodología aplicada, así como la integridad de la evidencia.
Ambos procesos deben de ser sistemáticos y respetar el orden de prioridad según la volatilidad de la información en los dispositivos originales. Para ello, los investigadores forenses cuentan con sus conocimientos como expertos y el conjunto de las buenas practicas ya comentadas.
En un plano más pragmático, se recomienda disponer de:

Registros cronológicos detallados de las actuaciones toma de datos de cualquier aspecto más o menos relevante, datos de interés que se identifiquen, que llamen la atención o sean significativos, o cualquier incidencia que surja durante el proceso.

Listas de chequeo éstas permiten seguir sin lugar a error los pasos esenciales identificando en cada paso los elementos susceptibles de contener información relevante.

En muchos casos, sólo existe una posibilidad de adquirir la evidencia, por lo que la adquisición se tiene que realizar adecuadamente, en la secuencia correcta y con todas las garantías necesarias.
La adquisición de datos puede darse en muy distintos escenarios a los que el analista forense se enfrentará, y que demandarán complejos y voluminosos procesos de copiado de datos que pueden requerir el uso de distintos medios, y para cada uno de ellos hay que aplicar métodos diferentes de tratamiento de la información. Por ejemplo, el:

- Escenario de copiado de disco o de archivos debe de garantizar que:
  - El original y la copia realizada deben ser idénticas.
    - Se debe de utilizar bloqueadores de disco, y dispositivos hardware y software que preserven la integridad del estado de los elementos de la escena.
    - Los medios de duplicación no deben de alterar la información contenida en la misma para preservar la originalidad y la integridad de la evidencia. Por ello se recomienda el uso de las herramientas hardware para realizar el procedimiento de copiado. Por ejemplo:
      1. Paraben
      2. Logicube
      3. ICS
      4. Data Device International
    - Si no se dispone de herramientas hardware, se recomienda el uso de 'dd' o 'dcfldd' para realizar el procedimiento de copiado.
    - Las dos opciones más normales de realizar una copia de un disco son la clonación del disco físico completo o de las unidades lógicas a otro disco físico lo más parecido posible, y la generación de un único fichero de imagen.
  - Para que un fedatario público (secretario judicial o notario, según el caso) pueda dar fe de lo acontecido y registrado en la actuación pericial es necesario registrar documentalmente y precintar las copias realizadas de las evidencias tomando las medidas legales necesarias.
  - Debe de evitarse alterar el origen ni el destino de los datos. Y en caso de que sea necesario, justificarlo adecuadamente.
    - La alteración de origen y destino de datos se puede dar más fácilmente en el entorno de red.
  - El copiado de discos debe ser completo, incluyendo el espacio que se conoce como 'slack' (espacio sobrante entre el final del archivo y el cluster que se considera usado, por lo que no es libre para ser utilizado por el sistema operativo) y el espacio libre.
    - Es interesante especialmente si se ha hecho uso de herramientas antiforenses ya que es posible que contenga información de interés.

- Escenario de captura de datos en red implica:
  - Asegurar que siempre se está trabajando dentro de las condiciones y requisitos de legalidad. No violar el contexto de privacidad que se debe preservar y contar con las autorizaciones adecuadas (legales y normativas de la empresa).

- Disponer de los medios y conocimientos para un controlar un contexto continuo en el tiempo y una compleja localización.
    - Un ejemplo es el seguimiento de accesos a dispositivos en red mediante el uso de dispositivos tipo sniffer.
- Se recomienda el uso de la herramienta 'NetCat' o 'nc' para la comunicación entre el equipo origen de los datos y el equipo utilizado por el analista forense.

- Escenario deslocalizado y descentralizado:

    - Es muy normal dentro del complejo mundo tecnológico actual desconocer la ubicación específica de los archivos o que éstos se encuentren ubicados en múltiples medios de almacenamiento.
    - En caso de no poder desplazar al investigador forense a las distintas localizaciones se podrá utilizar personal local como 'manos remotas', acceder por medios de comunicación remotos y trabajar sobre muestras más reducidas de las que se tomarían localmente.

Durante el proceso de identificación el investigador forense debe de haber recolectado toda la información requerida para la toma de decisiones durante el proceso de adquisición.

- Si el dispositivo está encendido ¿debe de mantenerlo encendido?
- Si el dispositivo está aislado de las comunicaciones, ¿cómo se debe de actuar para mantener su correcto aislamiento y preservarlo de actuaciones de terceros sin alterar la información contenida en el mismo?
- ¿Qué elementos o partes de los dispositivos puedan contener información relevante?
- En general es interesante no modificar el estado del dispositivo. Si éste se encuentra:

Apagado
- Realizar una copia bit a bit utilizando los métodos forenses adecuados.
- Certificar matemáticamente mediante un algoritmo Hash[7] la información obtenida.
- En caso de que sea necesario encenderlo, no hacerlo hasta haber realizado todas las copias necesarias, haberlas documentado, certificado y facilitado el registro al órgano competente.

Encendido
- Realizar copia bit a bit de todos los elementos que contengan información, aplicando el criterio de mayor volatilidad.
- Certificar matemáticamente mediante un algoritmo Hash la información obtenida.
- Previamente a la desconexión o al apagado de un dispositivo, se debe de evaluar:
    1. Las posibles implicaciones de desconectar el dispositivo de la red.
    2. La posibilidad de que sea accedido y manipulado por terceros durante la actuación pericial.

El investigador forense debe de disponer de las herramientas adecuadas para la correcta actuación en función de:

- Las particularidades de cada dispositivo.

[7] Las funciones hash transforman un mensaje de longitud arbitraria en un número fijo de bits, de tal forma que dos mensajes diferentes generaran dos secuencias HASH distintas.

- El proceso necesario seguir en cada caso.
- Los elementos de intercomunicación que se necesitan para interactuar con el dispositivo y realizar la copia.
- Los soportes necesarios para preservar la copia de las evidencias de los dispositivos.

Algunos de los conceptos a tener en cuenta seguro que suenan muy obvios, básicamente porque lo son, pero no por ello deben de ser omitidos en la metodología, ya que en muchas ocasiones el contexto de la investigación provoca errores en los aspectos más evidentes y en otros casos pueden resultar cuestiones obvias que, por simple desconocimiento pueden comprometer el resultado de la investigación. Es importante tener en cuenta que:

- En el caso de clonado de discos para su adquisición el disco destino deberá ser superior en tamaño al de origen.
- No es necesario clonar los dispositivos utilizando el mismo tipo de dispositivo, por ejemplo un dispositivo USB puede ser adquirido mediante una copia almacenada en un disco IDE o en otro dispositivo USB.
- El dispositivo de destino no debe de disponer de ningún dato previo. Si no se toma tal precaución es posible que en el espacio no copiado quedasen restos de datos de otros casos, con el consiguiente problema de mezcla de evidencias.
- Es importante etiquetar el dispositivo origen y el destino para su correcta identificación. Si por error se adquiere el contenido del dispositivo incorrectamente el investigador puede encontrarse con dos dispositivos vacíos y un gran problema para justificar su error frente al cliente.
- El investigador debe de tomar la decisión más adecuada a la hora de utilizar un método u otro de adquisición en función del escenario al que se enfrenta, el tipo de pruebas que sea necesario practicar y las herramientas disponibles para realizar el análisis. Por ejemplo, en una investigación donde hay una componente importante de análisis activo sería adecuado realizar un clonado de disco. Sin embargo, en el caso de que el objetivo de la investigación radique en buscar una determinada cadena de caracteres o un documento concreto, el método más adecuado, por su escasa complejidad, sería la generación de una imagen del dispositivo.
- Estimar el tiempo que es necesario dedicar para la adquisición de una evidencia depende de factores como el espacio a adquirir, la velocidad de los dispositivos, el tipo de soporte, el tipo de hash a realizar, si se va a realizar una verificación de copias, que junto a otros factores son elementos que influyen directamente sobre el tiempo de adquisición.

Es necesario preservar la trazabilidad y la integridad de la evidencia al realizar la entrega a otro investigador y obtener un recibo de entrega en custodia en la que se establezca que queda preservada, trasladada y continuada la Cadena de Custodia.

- Se realizará el levantamiento de acta por parte del fedatario publico tras realizarse, por parte del investigador, la entrega de:
    - La copia del documento de registro de los dispositivos.
    - Copias de las posibles evidencias.
- Se facilitará al analista copia del acta del fedatario publico de la entrega de material y documentación realizada como documentación de la actuación realizada.

- El investigador podrá realizar copias de las evidencias para su posterior análisis forense si ese es el objeto del encargo recibido por el mismo.

Finalmente, volver a recalcar que se tiene que registrar toda actuación realizada, detallando los pasos, el orden seguido, las copias realizadas, cómo ha quedado identificada cada copia, a quién ha sido entregada, como se da veracidad y fe de la misma, observaciones de interés que se hayan apreciado, y cualquier dato relevante para mantener la trazabilidad completa del proceso y de la evidencia.

- Cronología relacional o línea temporal (LT)

  La línea temporal es un concepto que ayuda al investigador a comprender la evolución de los hechos y la relación causa-efecto que existen en los mismos.

  La línea temporal consta de una sucesión de hechos indicados por algún indicio, como por ejemplo entradas en artefactos u operaciones no autorizadas de cualquier tipo (inicio de sesión en horario no autorizado, ejecución de un comando para abrir la conexión desde un host remoto, crear, borrar o modificar un archivo) que forman parte de una posible intrusión.

  La línea temporal se conforma a partir de todos aquellos elementos de evidencia que contienen información temporal fiable, ya sean marcas de tiempo (MAC) de ficheros, fechas y horas halladas en metadatos de ficheros de imágenes, datos de log del sistema, historial de navegación, etc.

  El procedimiento de creación de la cronología relacional es principalmente manual, sin embargo se pueden usar determinadas herramientas que faciliten la labor, extrayendo datos temporales del sistema y organizándolos de forma coherente y comprensible para los investigadores.

  La línea temporal, además de dar una perspectiva cronológica de los hechos, facilita el contexto del incidente, cuando se ha accedido a la información, se han modificado datos o se ha realizado el robo de contraseñas.

  En el caso de la documentación relativa a la cronología relacional no se ha considerado necesario la elaboración de una plantilla debido a su complejidad y el nivel de personalización que puede desarrollarse. Se trata básicamente de un listado en el que se debe de visualizar la cronología de los hechos.

  En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de documentación de la cronología relacional o línea temporal que puede servir como ejemplo para este tipo de documentos.

- Cadena de custodia (CdC)

  La *cadena de custodia* es un protocolo de actuación que se sigue para garantizar la validez de una evidencia, desde que ésta se obtiene hasta que se destruye o deja de ser necesaria, o de cualquier informe relativo a la misma. Con la particularidad, dado que nos encontramos en un entorno digital, de que la cadena de custodia no debe aplicarse sólo a aquellos dispositivos que se investigan en un momento dado. También debe aplicarse a aquellos datos que se generan sobre el terreno, de tal forma que tengan plena validez legal, ya sea como sustitución de una evidencia extinguida (como la pérdida de datos volátiles), o como apoyo a una prueba física.

  Si el investigador lo primero que hace es "desenchufar" los dispositivos es posible que elimine datos relevantes, sin embargo hay que desenchufar en algún momento.

  Este procedimiento de control debe ser absolutamente riguroso con la evidencia en todo su contexto, los hechos que la afectan y el personal que tiene acceso. Sin embargo, en informática, existe un conjunto de datos volátiles obtenidos en el primer análisis de los dispositivos que se destruyen irremediablemente. Esto implica que el investigador debe generar un informe basado en gran parte en la evidencia documental textual y fotográfica tomada en el momento de la primera investigación

realizada sobre el terreno, de todos aquellos datos que puedan ser obtenidos y que sabe que van a perderse nada más desenchufar el dispositivo. Por lo tanto, una muestra fotográfica del proceso de obtención de los datos volátiles y de las diferentes pantallas, así como de los datos característicos como el número de serie, modelo, forma física del mismo, y demás servirán para relacionar el continente con el contenido.

En el caso de la cadena de custodia no se ha considerado necesario la elaboración de una plantilla debido a su complejidad y el nivel de personalización que puede desarrollarse.

La documentación del protocolo controla dónde y cómo se ha obtenido cada evidencia, qué se ha hecho con ella, cuándo, quién ha tenido acceso a la misma, dónde se encuentra ésta en todo momento y quién la tiene y, en caso de su destrucción, cómo se ha destruido, cuándo, quién, dónde y porqué se ha destruido.

En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de cadena de custodia que puede servir como ejemplo para este tipo de documentos.

Proceso de preservación

En este punto ya se ha adquirido la evidencia digital.
La evidencia digital, tal como se ha comentado, es un elemento muy frágil, y puede ser eliminado o alternado apenas sin dejar rastro.
Las evidencias digitales son manipuladas durante todo el proceso, desde su adquisición hasta su posterior análisis. Es por esta razón que una de las premisas más importantes que se debe de respetar es no realizar actuaciones sobre la evidencia original, ya que la misma se podría eliminar, modificar o contaminar.
Continuando con las recomendaciones facilitadas en el apartado anterior, relativas al proceso de adquisición es de obligado cumplimiento, para la correcta preservación de las evidencias digitales que:

- El original y las copias realizadas deben ser idénticas.
- Debe obtenerse, como parte de la documentación, una 'función hash' que garantice que el disco o la información recolectada o adquirida no ha sido manipulada.
    - Se recomienda el uso de, al menos, una herramienta que utilice el algoritmo SHA-1 (Secure Hash Algorithm). Y de igual modo se desaconseja el uso de herramientas que utilicen el algoritmo MD5 (Message-Digest Algorithm 5).
    - Disponer del hash permite validar,ante la posible realización de análisis contrapericiales, que las actuaciones realizadas por el analista forense se realizaron sobre los datos originales y que los resultados obtenidos en dos momentos distintos del tiempo coinciden.
- Es recomendable realizar un mínimo de dos copias adicionales al original. Sin embargo, es mejor disponer de cuatro copias a repartir entre:
    - El investigador forense (2 copias, una de ellas se utiliza como imagen origen de todas las copias que sean necesarias).
    - La empresa u órgano de custodia (si lo hay).
    - El afectado por el caso.
- El disco original debe de ser salvaguardado utilizando las medidas adecuadas:
    - Almacenarlo por la entidad afectada con las garantías de seguridad debidas.
    - Depositarlo ante notario.

Como buenas prácticas relevantes, además de mantener un alto nivel de documentación para disponer de una trazabilidad clara e íntegra de los procesos realizados sobre cada una de las evidencias, se recomienda para la adecuada preservación de las evidencias:

- Utilizar guantes de látex durante todo el proceso.
- No modificar el estado de ninguno de los dispositivos sin haberlo documentado previamente.
- Asegurarse de mantener encendidos los dispositivos que ya lo estén, sobretodo los móviles, conectándolos a la alimentación si fuese preciso.
- Anular la conectividad de los dispositivos en la medida de lo posible, pero sin modificar el origen o destino de la información.
- Documentar, recoger y guardar adecuadamente los dispositivos de almacenamiento identificados.
- Tratar de que cualquier actuación sea repetible, y en caso de que no sea posible, disponer de las medidas necesarias para que sea aceptable como elemento probatorio en un proceso judicial.
- Guardar todo en un área asegurada.
- Asegurar que los elementos son guardados tomando las precauciones adecuadas, como el uso de bolsas antiestáticas, protectores antimagnéticos, anti-vibración, etc.

Proceso de análisis

Hasta el proceso de preservación, la industria dispone de buenas prácticas estandarizadas que permiten un entendimiento común entre los distintos profesionales, acerca de lo que se entiende como un comportamiento adecuado al enfrentar un proceso determinado. Éste no es el caso del proceso de análisis.
¡Por fin podemos hablar de los analistas forenses dentro de un contexto adecuado!
En la actualidad, la norma 'ISO/IEC 27042 - Tecnología de la información – Técnicas de seguridad – Directrices para el análisis e interpretación de la evidencia digital' se encuentra en desarrollo, y su publicación pretende marcar las directrices a seguir en el análisis e interpretación de la evidencia digital. En la norma, cuya publicación está prevista para el 28 de febrero de 2015, y de la que apenas hay información, se prevé que se trate en profundidad como hacer un análisis de la evidencia digital teniendo en cuenta los principios de validez, reproducibilidad, repetible, etc. Además, tratará el diseño e implementación de procedimientos de análisis que permitan ser revisados por un tercero cuando sea necesario e incluirá temas como la competencia personal que realiza los análisis, entre otros temas.
No es objetivo de este PFC realizar un amplio estudio de cómo analizar evidencias digitales, ya que este aspecto daría lugar a un estudio de mayor calado técnico y cuyo contenido sería indudablemente más extenso.
Por lo tanto, en el actual apartado voy a plantear una serie de buenas prácticas y consideraciones generales, que permitan la obtención de resultados adecuados en el proceso de análisis de las evidencias, basado en el conocimiento de distintos expertos en la materia.
En cualquier caso, dada su complejidad, al enfrentarse al proceso de análisis, es necesario valorar el escenario particular y sus peculiaridades ya que, en función de las mismas, deberá de identificar el modo de afrontar el mismo. Se podría completar un listado interminable con ejemplos objeto de análisis pericial y sus grandes diferencias.
Cualquiera que haya visto series de televisión como CSI querría ser analista forense digital (no creo que pase lo mismo con los médicos forenses, salvo que sea un miembro de la profesión).
Los casos relacionados con análisis de malware, análisis de memoria de dispositivos concretos, descubrimiento de técnicas antiforenses o de ocultación (como la estenografía) son ejemplos de escenarios excitantes e interesantes que se dan en la vida diaria de un analista forense digital.

Sin embargo, estas series sintetizan lo mejor y más entretenido de este trabajo, dejando de lado los aspectos más tediosos. En muchos casos, el trabajo del analista forense requiere el análisis de archivos de log interminables o la búsqueda de cadenas de caracteres entre un gran volumen de archivos o zonas de almacenamiento en disco menos accesibles.
Previo al momento de afrontar el análisis de evidencias, durante el proceso de preparación, se debe de haber obtenido del cliente la información de contexto que permita desarrollar las siguientes tareas de análisis:

- **Análisis de elementos o palabras clave**
    - Si durante el análisis de los datos disponibles los indicios no estarán definidos con claridad, se debe de solicitar una orientación adicional al respecto de qué buscar.
    - Ejemplos de elementos clave que suelen ser datos que el cliente puede llegar a facilitar son, un nombre, una URL, una dirección de correo o un teléfono.
    - Sin estos datos es muy complejo realizar una investigación en mayor profundidad.
- **Análisis de actores y cuadro relacional**
    - Verificar y analizar, conjuntamente con el resto de información disponible, si se dispone de los actores principales:
        - Personas, equipos, programas y demás elementos potencialmente involucradas.
        - 'Alias' de las personas potencialmente involucradas.
    - Interacción: información de los acceso y de los registros, donde, cuando, con que frecuencia, que información es de cada usuario, accesos a los equipos, permisos de trabajo y privilegios, etc.
        - Se recomienda definir un cuadro relacional.
- **Cronología relacional o línea temporal del suceso a investigar**
    - Acotar la investigación en términos temporales.
    - Elaborar una línea cronológica de los acontecimientos, de su interpelación y vínculos a lo largo del tiempo.
    - Asocia evidencias que permiten relacionar los distintos elementos de prueba a la línea cronológica desarrollada, y de este modo, sustentar las posteriores conclusiones.
    - Sustenta las conclusiones, muchas de las cuales se apoyarán en información de fechas y horas, siguiendo patrones claramente definidos.

Otra de las primeras tareas a realizar por parte del analista es el desarrollo de los checklist de herramientas y artefactos (descritos más adelante) en función de la información disponible acerca de los distintos elementos a analizar.
Las labores de análisis no son tareas que finalizan secuencialmente y tras el desarrollo de un documento. Normalmente, una vez se dispone de una serie de datos iniciales, las labores de análisis son tareas en paralelo que en muchos casos se retroalimentan o se complementan para dar lugar a distintos resultados. No es posible asignarles un tiempo para su completo desarrollo, por lo que es necesario acotarlas en tiempo asumiendo que se trabaja en modo 'best effort', y eso es algo muy importante a trasladar al cliente. Cuanto más tiempo se pueda dedicar al análisis, mejores o más acertadas serán las conclusiones expuestas en el informe.
En general, el proceso de análisis de una evidencia digital:

- Nunca debe de aplicarse sobre los medios originales o sobre la copia en custodia de los anteriores, sino sobre la copia extraída de éstas últimas, que seguirá utilizándose para realizar sucesivas copias cuando sean necesarias.
- Debe de estar basado en el método científico, ser metódico, sistematizado, y plantear hipótesis obteniendo evidencias que la refrenden.
- Debe permitir el análisis de la información que permita llegar a la obtención de las conclusiones sobre lo que se desea conocer o determinar.
- Debe plantearse con amplitud de miras, evitar la posible pérdida de evidencias por haber circunscrito la investigación al marco operativo e indicios originales exclusivamente.
- Nunca debe descartar la posibilidad de incorporar nuevas evidencias a un escenario.
    - Cuando la existencia de un caso pasa a ser pública, es habitual la eliminación de evidencias por parte de los afectados.
- Tiene que ser muy cuidadoso con el tratamiento de aquellos datos que puedan afectar a la intimidad de las personas objeto de investigación.
- Debe de contemplar la detección de patrones de conducta.
    - Contrastar los patrones obtenidos con el cliente.
        - Sin embargo, hay que tener en cuenta que las conclusiones del analista forense nunca puede encontrarse condicionado por el cliente.
        - Es tarea del analista forense solicitar la información que necesite y, atendiendo a su criterio, llegar a las conclusiones que considere.
    - Ejemplos de patrones que pueden ser fáciles de rastrear son:
        - Frases o palabras especiales.
        - Usuarios que se conectan a horas concretas.
        - Correos que se envían desde direcciones IP específicas que, aunque dinámicas, pertenecen a un mismo rango.
- Debe ser extremadamente escrupuloso e inevitablemente esto implica ser organizado.
    - Saltar de una evidencia a otra sin una visión clara se reflejará sobre el informe resultante.
- Debe anotar cualquier apreciación relativa a información obtenida directamente o a partir del cruce de resultados.
    - Un error muy común es confiar en las capacidades de memoria personales.
    - Debe llevar un cuaderno de bitácora (puede ser un archivo electrónico o una libreta) donde anotar cualquier apreciación, evidencia, horas, fechas, nombres o cualquier dato o impresión que pueda considerarse de interés.
- Las herramientas no utilizadas de forma adecuada serán de escasa o nula utilidad. La experiencia ha mostrado lo potentes que pueden llegar a ser aplicaciones sencillas utilizadas por manos expertas.
- No existen varitas ni teclas mágicas para afrontar en un caso la fase de análisis. Cada uno de ellos presenta sus peculiaridades y es muy importante desprenderse desde un principio de prejuicios y conclusiones preconcebidas.

- No debe olvidarse tampoco, que en ocasiones la visión profesional de un tercero puede dar aire fresco a la investigación en momentos de bloqueo de ésta.
- Es directamente dependiente de la experiencia y efectividad del analista forense, ya que éstos son la clave para obtener resultados válidos y fiables.
- Debe de llegar a conclusiones rotundas, difícilmente refutables.
- Como curiosidad, a continuación he seleccionado algunas frases que creo realmente relevantes, escritas por el escritor inglés Arthur Conan Doyle (1859–1930) y que puso en boca de Sherlock Holmes, un detective ficticio (y en mi opinión un gran investigador / perito / analista) creado por él:
    - 'Datos, datos, datos. No puedo fabricar ladrillos sin arcilla'.
        - Quizás una de las mejores frases que se han escrito en referencia a una investigación. Es algo evidente, o debería de serlo, que sin datos es imposible realizar una investigación.
    - 'Nada resulta más engañoso que un hecho evidente'.
        - Si bien ésta afirmación contradice el principio de parsimonia o navaja de Ockham, que dice que 'en igualdad de condiciones, la explicación más sencilla suele ser la correcta'.
    - 'Watson, no hay que suponer si no tenemos evidencia'.
        - Las ideas preconcebidas que no están soportadas en evidencias son un error en si miasmas.
    - 'Es un error capital el teorizar antes de poseer datos. Insensiblemente, uno comienza a deformar los hechos para hacerlos encajar en las teorías en lugar de encajar las teorías en los hechos.'
        - Buscar resultados rápidos implica cometer errores ya que la investigación pasa a ser una teorización, y en teoría, casi todo es viable, pero lo más probable es que la teoría no se alinee con la realidad.
    - 'Cuando eliminas toda solución lógica a un problema, lo ilógico, aunque imposible, es invariablemente lo cierto.'
        - Al hilo de la frase anterior, cuando basándose en evidencias, la única teoría se identifica como improbable, es muy probable que sea la correcta. Al fin y al cabo se basa en evidencias.
    - 'Nunca hago excepciones; la excepción invalida la regla'.
        - En el momento que se hace una excepción entramos en terreno de 'todo vale', ya que eliminamos elementos de juicio objetivos de forma subjetiva.
    - 'Al contrario, Watson, lo tiene todo a la vista. Pero no es capaz de razonar a partir de lo que ve. Es usted demasiado tímido a la hora de hacer deducciones'.
        - El analista forense nunca debe de dejarse influir por condicionamientos externos.
    - 'Usted, Watson, está interpretando la situación desde el punto de vista de Lestrade'.
        - La influencia de terceras personas puede ser muy negativa, ya que el responsable de una investigación en el propio investigador, y sobre él recae la responsabilidad final.
    - 'No existe una combinación de sucesos que la inteligencia de un hombre no sea capaz de explicar.'

    - La correlación de eventos es muy compleja, sin embargo, con el conocimiento suficiente y los eventos adecuados, el llegar a conclusiones coherentes y acertadas es cuestión de tiempo y esfuerzo.

Cada análisis es único en función de parámetros como antecedentes conocidos, objetivo, medios, evidencias recolectadas y el estado de las mismas.
En algunos escenarios concretos, como es el caso de los dispositivos móviles , existe documentación acerca de buenas prácticas o técnicas de análisis. La web del NIST es una buena fuente de documentación para disponer de algunos procedimientos gratuitos, y adicionalmente, previo pago, otras organizaciones han desarrollado documentación relativa a diferentes temas como:

- Sistemas operativos.
- Medios de almacenamiento de información.
- Tipología de la información (ficheros gráficos, de ofimática, log y trazas, registros, volcados de información capturada, etc.).

Si bien al analista forense le llega toda la información recuperada, en muchos casos va a ser necesario aplicar técnicas y herramientas específicas de reconstrucción de información debido a acciones de borrado, formateo o simplemente daños accidentales, así como para completar la información relevante de cada archivo, como pudieran ser los metadatos del mismo, que permiten conocer aspectos como el ciclo de vida del mismo, fechas y horas de la creación, accesos, modificaciones, y otra información de interés en función del origen. Por otro lado, en función del estado de la información, es recomendable contar con los servicios especializados de expertos en este tipo de actividades.
En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de documentación del proceso de análisis que puede servir como ejemplo para este tipo de documentos.

- Checklist de herramientas hardware y software (CHS)

  El checklist de herramientas hardware y software no forma parte de la documentación propia de la investigación, sino que se trata de documentación específica de cada investigador.

  Este documento permite al investigador preparar mejor la investigación dado que identificar la necesidad o la falta de una herramienta específica durante un momento clave de la investigación puede derivar en problemas importantes para la misma.

  Adicionalmente, este documento permite al investigador seleccionar las herramientas adecuadas en cada caso, y, adicionalmente, documentar el uso específico de cada una de ellas en casos concretos que pueden ser utilizados posteriormente.

  En este punto se sobreentiende que no se trata de un checklist al uso, al estilo de los simples listados, sino que su utilidad va más allá, permitiendo al investigador reutilizar el conocimiento adquirido puntualmente en casos posteriores.

  En el caso de los checklist de herramientas hardware y software se ha elaborado una plantilla de checklist de herramientas, si bien el nivel de personalización que puede desarrollarse es muy grande.

  Se trata básicamente de un listado en el que se deben de documentar los aspectos citados y cualquier aspecto adicional relativo al uso de los mismos, como enlaces a manuales de uso, 'howtos', tiendas donde adquirir recambios, o cualquier conocimiento que pueda resultar relevante a la hora de trabajar con las distintas herramientas.

  En el capítulo dedicado a la prueba de concepto se desarrolla un checklist de herramientas hardware y software que puede servir como ejemplo para este tipo de documentos.

- Checklist de artefactos (CHA)

  El checklist de artefactos, al igual que el checklist de herramientas hardware y software, no forma parte de la documentación propia de la investigación, sino que se trata de documentación específica de cada investigador.

  Este documento permite preparar mejor la investigación dado que ayuda al investigador a dirigir la investigación hacia los elementos en los que normalmente se identifica la información crítica de los sistemas y que finalmente puede ser tratada como evidencia si así lo estima el investigador.

  En muchos casos el investigador, a raíz de los antecedentes y la información recabada, identifica los elementos críticos a analizar. Sin embargo, existen muchas otras ocasiones donde no es tan evidente el objeto de investigación y se debe de iniciar la misma investigando los artefactos más relevantes del sistema, sin tener la seguridad de si son los más adecuados.

  Este documento permite al investigador seleccionar los artefactos más adecuados en cada caso, y, adicionalmente, documentar el uso específico de cada uno de ellos en casos concretos que pueden ser utilizados posteriormente.

  En este punto se entiende que no se trata de un checklist al uso, al estilo de los listados, sino que su utilidad va más allá, permitiendo al investigador reutilizar el conocimiento adquirido puntualmente en casos posteriores.

  En el caso de los checklist de artefactos no se ha considerado necesario la elaboración de una plantilla adicional al anterior debido a su escasa complejidad y el nivel de personalización que puede desarrollarse. Se trata básicamente de un listado en el que se deben de documentar los aspectos citados y cualquier aspecto adicional relativo al uso de los mismos, como enlaces o cualquier conocimiento que pueda resultar relevante a la hora de trabajar con los distintos artefactos.

  En el capítulo dedicado a la prueba de concepto se desarrolla un checklist de artefactos que puede servir como ejemplo para este tipo de documentos.

  Adicionalmente, en la web de Enisa podemos encontrar mucha documentación relativa a artefactos que podemos reutilizar para iniciar nuestra propia documentación.

Proceso de consolidación

El análisis de las evidencias, permite al investigador (efectivamente, de nuevo se trata del investigador, ya que es posible que no sea el analista el responsable de desarrollar los informes) llegar a una serie de conclusiones determinadas que deben quedar reflejadas en el informe de análisis forense.
Normalmente se utiliza indistintamente las palabras 'informe' y 'dictamen' cuando semánticamente son distintos.

- Informe (De informar):

  1. m. Descripción, oral o escrita, de las características y circunstancias de un suceso o asunto.
  2. m. Acción y efecto de informar (‖ dictaminar).
  3. m. Der. Exposición total que hace el letrado o el fiscal ante el tribunal que ha de fallar el proceso.

- Dictamen (Del lat. *dictmen*):

  1. m. Opinión y juicio que se forma o emite sobre algo.

La confusión a la hora de utilizarlos se debe a que en los informes es común expresar opiniones y juicios. El informe forense debe de tener un enfoque claro, preciso y compresible por terceras personas que no estén relacionados con el tema e incluso para personas no expertas en la materia. Sin embargo, al mismo tiempo, tiene que contener la información técnica suficiente para poder ser comprendida por técnicos especialistas en la materia.
Para el desarrollo del contenido técnico es aconsejable que aparezca en los anexos, de forma que el desarrollo de la información haga referencia a los mismos, pero que no interfiera en la comprensión de los lectores sin capacidades técnicas.
Otra opción es desarrollar dos documentos:

Informe de Resumen ejecutivo Informe diseñado para proporcionar al lector la información más crítica, un análisis sin desarrollar los aspectos técnicos y conclusiones objetivas e imparciales.

Informe técnico Informe exhaustivo en el detalle de la información técnica y metodológica, en el que se desarrollan las conclusiones extraídas del análisis de las evidencias y sustentadas por las mismas, y no se expresan juicios u opiniones parciales.

Es recomendable, a la hora de desarrollar un informe, apoyarse en documentos de referencia o protocolos como la `norma UNE 197001:2011` explicada anteriormente.
Otra alternativa a la hora de desarrollar el informe es utilizar una plantilla o herramienta desarrollada a tal efecto por un tercero. A este respecto, he encontrado estamentos públicos y empresas que desarrollan plantillas básicas que ponen a disposición de los usuarios, pero están muy vinculadas con la legislación del país origen[8]. Una herramienta ampliamente reconocida que permite desarrollar un informe una vez finalizada la investigación es FTK (Forensic Toolkit), que, como se puede ver en la imagen, dispone de un módulo de informes.

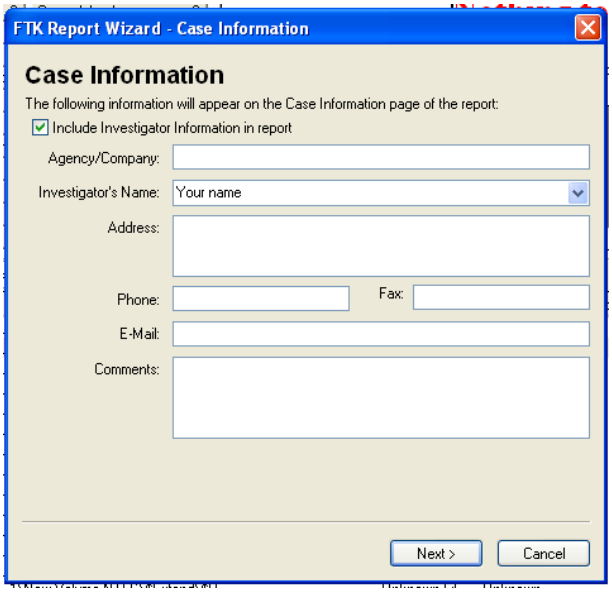


Figura 2: Informes con FTK

En última instancia es responsabilidad del investigador forense la elaboración del informe y éste dispone de total libertad para la redacción del mismo en cuanto a formato, estructura y contenido.
Algunas recomendaciones recabadas de la documentación estudiada y que no han sido nombradas explícitamente, o que considero importante repetir, son:

[8]Por ejemplo `http://i-sight.com/investigation/investigation-report-essentials/`.

- Especificar la razón concreta por la que el cliente contacta con el analista forense para proponerle el proyecto.
- Especificar claramente la línea temporal del proyecto.
- Enumerar las evidencias (si se dispone de fotografías, el número debe de aparecer al lado) facilitando además sobre ellas toda la información posible.
- Definir en el informe los fundamentos que demuestren la no manipulación de las evidencias, el porqué de la metodología empleada, ahondando en las precauciones que se han tomado y su importancia con respecto al caso.
- El 'Principio de intercambio' formulado por Locard afirma que 'siempre que dos objetos entran en contacto transfieren parte del material que incorporan al otro objeto'.
- El exceso de información es tan grave como la falta de la misma, ya que puede desembocar en desinformación o falta de claridad.
- La identificación de patrones de comportamiento deben citarse como un aspecto importante a la hora de elaborar las conclusiones.
- Siempre que sea necesaria, podrá establecerse la correlación existente entre los distintos análisis.
- Los datos deben ser el hilo conductor de la investigación, realzando los más significativos.
- El análisis debe reflejar la pericia del analista forense así como la eficacia de los métodos y aplicaciones empleadas.
- Las conclusiones son uno de los apartados finales del informe, sin embargo muy probablemente será el punto que se lea en primera instancia.
- El analista debe de abstraerse de las circunstancias externas del caso, sin que las consecuencias posteriores que las conclusiones de su labor pueden acarrear afecten a su juicio.
- Lo mejor son pocos argumentos bien planteados.
- No es objetivo del analista elucubrar sobre las posibilidades que pueden aportar datos no analizados por alguna circunstancia ajena al analista, pero sí debe de reflejar en el informe que a partir de ellos podría ser posible ampliar las conclusiones.
- `http://static.eluniversal.com/2008/05/15/infointerpol.pdf`
    - Ejemplo de informe pericial de carácter 'oficial" elaborado por la Interpol sobre los ordenadores y equipos informáticos de las FARC decomisados en Colombia.

Previo a la entrega del informe definitivo, se recomienda tener una reunión con el cliente, explicar el contenido del informe y aclarar cualquier duda que pueda surgir. Esto facilitará la comprensión del contenido del mismo por los interesados. Sin embargo, de nuevo, hay que insistir en la independencia de analista, por lo que lo acontecido en dicha reunión no debe de afectar a las conclusiones del mismo.
Finalmente, el investigador forense debe de mantener bajo su propia custodia una copia del informe entregado así como las trazas de los análisis y pruebas realizadas durante la actuación que le permitan recordar, en cualquier momento, todo lo necesario como para trasladar sus conclusiones sin ninguna sombra de duda.
¿Para qué es necesario seguir un proceso adecuado y desarrollar la documentación descrita?

Supongamos que, como analista forense, me encuentro ante la necesidad de presentar mi análisis a un Juez explicando que, por ejemplo, a través del análisis de la memoria RAM de un equipo corporativo se ha identificado una dirección de memoria que permite tener constancia de la manipulación de un proceso del sistema que interfiere en las pulsaciones del teclado. Y que, además, dicha manipulación se produjo por la instalación de una aplicación que, aunque en el registro del sistema aparezca realizada por el usuario demandante, se cree que en realidad fue llevada a efecto por el demandado, mediante una intrusión en el sistema del usuario demandante a través de una vulnerabilidad en la máquina virtual de Java del equipo del mismo.
Tras la experiencia laboral de presentar un informe forense claro y conciso, en el que sólo había que entender el concepto de dirección IP a nivel usuario y que el Juez, tras no enterarse de nada, ordenase tomar nota de dicha dirección sin los puntos que separan los cuatro octetos, es inmediato deducir que la posibilidad de transmitir la información del caso anteriormente planteado a un juez, y que comprenda mínimamente el contexto para tomar una resolución, es una labor casi imposible.
Sin embargo, un informe completo, descriptivo, profesional, riguroso, respetuoso y argumentativo, junto a una buena cronología acompañada de un mapa relacional y conservando copia de todo lo necesario para poder, en un momento dado, rememorar todo el proceso y las actuaciones, siendo capaz de realizar una exposición o dar las pertinentes explicaciones en un tribunal, pueden permitir al Juez entender mejor la situación desde un plano menos técnico, como ha transcurrido la misma y con ella determinar cuales son los momentos importantes y las evidencias que pueden refrendar o aportar información sobre lo acontecido.
En definitiva, y a pesar de lo descrito anteriormente, en muchas ocasiones, un analista forense tiene que hablar de 'interpretaciones', como asociar el concepto de dirección IP a la dirección postal de una vivienda, en lugar de hechos claros, ante lo cual serán los datos más simples y asequibles, alejados de complejos planteamientos técnicos los más útiles para la labor tanto de analistas forenses como abogados.
Finalmente, una vez se ha acordado con el cliente el fin de la investigación, es necesario que se firme el documento de aceptación de fin de proyecto.

- Informe de resumen ejecutivo (IRE)

  El resumen ejecutivo es un documento diseñado para proporcionar al lector la información más crítica, un informe que presente conclusiones objetivas e imparciales pero sin desarrollar los aspectos técnicos.

  En el caso del resumen ejecutivo no se ha considerado necesario la elaboración de una plantilla debido a su complejidad y el nivel de personalización que puede desarrollarse.

  En el capítulo dedicado a la prueba de concepto no se desarrolla un ejemplo de resumen ejecutivo ya que, al desarrollarse en informe técnico completo, el desarrollo de otro informe adicional no aporta ningún valor adicional al proyecto.

- Informe técnico forense digital (IFD)

  El informe forense digital es el documento que consolida toda la labor de investigación, debe de ser exhaustivo en el detalle de la información técnica y metodológica, en el que se desarrollan las conclusiones extraídas del análisis de las evidencias y sustentadas por las mismas, y no se expresan juicios u opiniones parciales.

  Tal como se ha comentado es recomendable seguir las recomendaciones de la norma UNE 197001:2011 'Criterios generales para la elaboración de informes y dictámenes periciales'.

  Además, los responsables del reto forense facilitan la siguiente estructura para el informe a presentar, que si bien no sigue el estándar internacional tiene algunas similitudes como se puede observar:

1. Introducción
   1. Antecedentes del incidente
   2. Objetivos de la investigación
2. Entorno de investigación

   El propósito de este capítulo es detallar las herramientas empleadas en el análisis, así como la construcción del entorno de análisis forense usado para la investigación.

3. Proceso de análisis

   En este apartado se detalla de forma resumida la secuencia de actividades llevada a cabo para la obtención de las evidencias objeto del análisis. Debido a la limitación de espacio, su exposición es muy sintética, puesto que relatar en detalle todas y cada una de las acciones realizadas llevaría aparejada mucha más información.

4. Cronograma de actividades

   El objeto de este capítulo es mostrar todas las actividades realizadas por el (los) atacante(s) de una forma secuencial, desde el inicio de las mismas hasta la realización de la imagen del sistema, añadiendo en cada punto la evidencia que lo sustenta.

   1. Diagrama temporal

   Asimismo, a continuación, se muestra en forma de diagrama una representación en el tiempo de la intrusión. Se muestra así de un vistazo qué es lo que hizo el atacante y cuándo lo hizo.

5. Análisis de artefactos

   En este capítulo se analizan todos los ficheros creados en el sistema como consecuencia del ataque, indicando su objetivo y cualquier otro dato de interés relativo a los mismos.

6. Direcciones IP implicadas

   Se refleja aquí la información obtenida sobre las direcciones IP que de una u otra manera se han visto implicadas en el incidente, incluyendo la de quien ó quienes atacaron el sistema.

7. Alcance de la intrusión

   En este apartado se resume hasta qué punto la intrusión afecto al sistema y a la información en él alojada.

```
8. Conclusiones

   Este apartado aglutina los principales puntos que se obtienen
   como consecuencia del análisis efectuado.

9. Recomendaciones

   Finalmente, este apartado enumera algunas recomendaciones para
   solucionar la actual situación y para prevenir situaciones
   similares en el futuro.

10. Referencias

11. Anexos
```

En el caso del informe forense digital no se ha considerado necesario la elaboración de una plantilla debido a su complejidad y el nivel de personalización que puede desarrollarse, pero se han desarrollado una serie de recomendaciones que se exponen a continuación.

```
Es muy importante recordar que el informe debe de alimentarse de la
documentación anteriormente generada a lo largo de toda la investigación
y que cualquier información debe de estar refrendada por la
documentación, pruebas y resultados obtenidos hasta el momento de la
redacción del presente informe.
```

En el capítulo dedicado a la prueba de concepto se desarrolla un ejemplo de informe forense digital que puede servir como ejemplo para este tipo de documentos, y que sigue las recomendaciones descritas a continuación:

- Documento
  - Paginación: Todas las páginas deben estar numeradas.
  - Cabecera/Pie:
    - Título
    - Código de ref
    - Fecha de liberación del informe
    - Numeración (x de y)
- Portada
  - Título
  - Cod. de expediente/procedimiento (si existe)
  - Datos del peticionario de la actuación
  - Datos del destinatario del informe
  - Datos del investigador
  - Datos del letrado (si procede)
  - Datos de la localización física del análisis (Dirección, Coordenadas GPS o UTM, enlace a Google Maps.)

- Declaración de tachas

  El analista forense debe de expresar por escrito que actúa de buena fe y que no existe ningún motivo por el cual deba de abstenerse de realizar el informe.

- Juramento o promesa

  El informe pericial no puede ser desarrollado por una persona relacionada con el proceso. El analista debe de ser independiente y objetivo, además de poseer los conocimientos necesarios para desarrollarlo.

  Este texto es en cierto modo irrelevante, ya que el mero hecho de aceptar el trabajo de realizar el informe conlleva las obligaciones que desarrolla ésta declaración. La misma implica que el analista forense:

  - Está procediendo bajo juramento o promesa de decir la verdad, y haber actuado con la mayor objetividad e imparcialidad posible.
  - Está en conocimiento de las sanciones penales de no actuar de ese modo.

- Índice general

  En el presente apartado se explica que su objetivo es facilitar la búsqueda y localización de la información por los diferentes capítulos.

  Se debe de incluir el esquema básico del informe, que se compone de los títulos y numeración de los puntos más relevantes del informe llegando a la profundidad que el analista forense considere, siempre que se respeten las normas de simplicidad y claridad.

  Este apartado se corresponde con el apartado de 'Objetivos del reto' del informe técnico del reto.

- Cuerpo del informe

  Los puntos a desarrollar son:

  - **Objeto**. Aclara la finalidad del informe forense, e introducir qué es lo que se pretende con todo el trabajo realizado.
  - **Alcance**. Tal como indica su título, en este apartado se desarrolla el alcance de cada una de las cuestiones que se plantearon en el apartado anterior de forma que quede claro para el receptor del informe que se ha cumplido con los objetivos acordados, y, en caso de que el alcance se haya modificado durante el desarrollo del proyecto (siempre de mutuo acuerdo), que todo aparezca claramente reflejado. Además, se desarrollarán aspectos como los procesos, recursos, limitaciones, esfuerzo y presupuesto.
  - **Antecedentes**. Son los hechos acontecidos con anterioridad al inicio del análisis forense y que sirven de punto de partida del mismo.
    Sin embargo, los antecedentes no deben de condicionar el resultado del informe, y deben de tomarse como una fuente más de información que debe de ser tratada.
  - Consideraciones preliminares. Dado que el informe se desarrolla a posteriori, al redactar este apartado conocemos lo que pensábamos, como analistas previo a realizar el análisis y la certeza o errores de nuestras consideraciones previas. Aquí se desarrolla todo lo que el analista forense considere necesario para explicar las decisiones tomadas en función de la información que se tenía en ese momento, como se desarrolló el trabajo, qué bases teóricas dieron lugar a la utilización de una u otra tecnología, los procedimientos seguidos, así como las limitaciones y restricciones que existieron en cada momento.
    Toda esta información permitirá conocer y entender como se ha realizado el trabajo, porque se ha identificado y extraído determinadas evidencias y otras se han podido perder, y cómo se ha llegado a las conclusiones presentadas.

- **Documentos de referencia**. Libros, documentos, manuales, normas, información obtenida de URLs, etc. Cualquier soporte, físico o electrónico, que haya sido utilizado para desarrollar el análisis forense.
- Terminología y abreviaturas. Todos los términos tecnológicos y abreviaturas que se han usado en la redacción del informe.
- **Proceso de análisis**
  - **Actuaciones**. (Equivale al proceso de análisis del informe del reto) Cada acción que ejecuta el analista forense debe de estar justificada previo a realizarla, y documentada durante todo el proceso, de modo que el analista forense se encuentre en disposición de contestar cualquier cuestión que se le plantee posteriormente.
    Este apartado es especialmente importante el las actuaciones complejas, ya que la memoria no es fiable.
  - **Análisis**. (Equivale al análisis de artefactos). Toda la labor realizada por el analista debe de quedar, de la forma más explícita y resumida posible, plasmada y justificada en este apartado.
    Debe de aparecer reflejado todo el proceso, fundamentado en buenas prácticas o experiencias previas a falta de las primeras, todas la situaciones que se han ido dando, la resolución de las mismas y cualquier explicación que permita comprender, sin lugar a dudas, el porque de cada paso dado y su necesidad.
    Para toda aquella información que sea demasiado extensa o técnica se tendrá que evaluar la necesidad o idoneidad de que aparezca en este apartado o en los anexos, haciendo referencia a los mismos.
- **Cronología de eventos**
- **Línea temporal**
- **Conclusiones**. (Incluye el alcance de la intrusión). Sólo deben de desarrollarse las conclusiones de las cuestiones planteadas. Ésas deben de ser:
  - Objetivas.
  - Precisas.
  - Claras.
  - Justificadas.
- **RECOMENDACIONES**
  - En caso de que se soliciten como parte de la investigación digital. En un proceso forense no son necesarias ya que no forma parte del alcance.
- **ANEJOS**. No existen normas predefinidas para este apartado. Cualquier aspecto que, por la razón que sea, no haya podido ser desarrollado a lo largo del informe se puede y debe de añadir en como anexo y deben de formar parte del mismo como cualquier otro punto, e incluirlos en el índice.
  - **Direcciones IP implicadas**
  - **Cualquier documento**, nota, fotografía que ayude a entender o reforzar el contenido de la pericial.
  - Temas técnicos tratados en profundidad.
  - Descripción de los méritos, menciones, titulaciones y certificaciones, experiencia y trayectoria que acreditan al analista forense como experto en la materia sobre la que se ha realizado el informe.
  - Datos relativos a la fecha de solicitud del informe, el plazo dado para la realización del mismo y cualquier evento que haya podido modificar en el tiempo los resultados del análisis, como retrasos justificados o injustificados.

- Documento de aceptación de fin de proyecto (AFP)

  El documento de aceptación de fin de proyecto debe de ser firmado por el cliente cuando el mismo considere finalizada la investigación.

  El objetivo del documento es dejar por escrito la aceptación del correcto cierre de la investigación. Este documento debe de ser el origen de las respuestas ante cualquier duda o problema con el cliente acerca del correcto cierre de la investigación.

  En el documento, además de concretar los datos que permitan identificar la investigación, se deben especificar los datos del cliente, la fecha de fin y la firma de aceptación del cliente.

  A continuación se presenta una posible plantilla que se ha desarrollado y adaptado para su uso mediante Emacs tal y como se puede ver a continuación:

  Documento de aceptacion de fin de proyecto.org

Herramientas forenses propuestas

Al llegar a este punto se ha facilitado al lector las bases metodológicas necesarias para el adecuado desarrollo de un proyecto forense dentro de las prácticas legalmente establecidas.
El objetivo de este capítulo es plantear una posible forma de uso de distintas herramientas desde Emacs para obtener información relevante para la investigación en un proyecto de análisis forense. En ningún caso trata de explicar detalladamente para que se utilizan las distintas aplicaciones que se van a utilizar.
En caso de que el lector desconozca la utilidad de alguna de las herramientas propuestas se recomienda consultar los enlaces que se proporcionan integrados en el texto.
Uno de los aspectos clave a tener en cuenta durante un análisis forense es no alterar el escenario objeto de análisis. Sin embargo, en muchas ocasiones no es una alternativa, por lo que la cuestión principal es realizar el menor número de alteraciones posibles y controlar y documentar todos los pasos realizados.
Con las premisas establecidas, las herramientas utilizadas serán lanzadas desde línea de comando de modo que minimicen la modificación del estado del sistema en cualquier aspecto y lo menos intrusivas posible.
Por otro lado, no es adecuado utilizar las herramientas propias del sistema analizado ya que éstas pueden estar manipuladas y ofrecer datos erróneos. Incluso utilizando herramientas externas al sistema analizado, algunos rootkits que trabajan a bajo nivel pueden devolver datos erróneos.
Se recomienda disponer de algún tipo de soporte de almacenamiento externo que contenga todas las herramientas , plantillas y cualquier archivo que pueda requerir el análisis tal como se ha comentado anteriormente.

Tipos de análisis y herramientas

Se ha comentado en varias ocasiones la importancia de llevar a efecto un proceso controlado (tal y como se ha descrito en el tema relativo a metodologías) y herramientas adecuadas para la adquisición de evidencias.
Además de herramientas, algunas de las cuales serán utilizadas en el PFC, existen distintas suites orientadas al análisis forense que han evolucionado en el tiempo. Algunas de las más utilizadas son:

- Caine
- Helix
- deft
- SANS Investigate Forensic Toolkit (SIFT)

- Matriux
- Masterkey
- Plainsight

Estas distribuciones, basadas en Live distros ofrecen funcionalidades para realizar análisis **live forensics**, **logical acquisition**, **sparse acquisition** y **post mortem**.
El análisis **live forensics** o **live acquisitions** se fundamenta en la obtención de evidencias y análisis de un equipo *mientras el sistema operativo se encuentra en funcionamiento*. Este tipo de análisis resultan especialmente adecuados en escenarios relativos a la identificación de aplicaciones con código malicioso o de ataques que se producen en red. Dado que en este tipo de situaciones existe una alta posibilidad de alterar las evidencias es especialmente crítico realizar las copias de seguridad y volcados de datos necesarios previo al inicio de la investigación.
Dada la complejidad del tipo de análisis anterior a la hora de mantener la integridad del sistema, y en consecuencia la integridad de las evidencias, el tipo de investigación forense más frecuente es el análisis **post mortem**, que se realiza sin arrancar el sistema operativo del equipo a analizar. En este tipo de investigación el riesgo de modificación de evidencias es muy bajo, y se dispone de los elementos necesarios para volver a realizar las pruebas en caso necesario. Este tipo de investigación es especialmente útil para búsquedas de datos, análisis de registros o recuperación de ficheros eliminados, por citar algunos ejemplos significativos.
Cuando se trata de identificación de archivos concretos, como la búsqueda de logs, archivos de correo electrónico u similar, el método utilizado es **logical acquisition**, y si dentro del ámbito de este tipo de análisis se contempla la recuperación de ficheros borrados, al mismo se la identifica como **sparse acquisition**.
En cualquiera de los tipos enumerados las fases a seguir y las medidas a contemplar son las mismas o muy similares. A continuación, para cada una de las fases ya desarrolladas en la metodología, se presentarán una serie de herramientas que permiten el desarrollo de cada una de las mismas.

Escenarios

El uso de Emacs es muy similar en los sistemas operativos objeto del alcance del presente PFC: Linux, windows y MacOS.
Si bien todos los sistemas operativos disponen de herramientas para la ejecución de distintos test, como se puede observar en el apartado anterior, los sistemas Linux disponen de un mayor abanico de herramientas que el resto, por lo que se recomienda su uso.
Hay tres escenarios básicos a la hora de plantear la investigación de un equipo:

1. Análisis local de la máquina.
2. Análisis remoto de la máquina.
3. Análisis de dispositivo de almacenamiento.

En particular, el análisis local puede darse en dos modalidades:

- Análisis de la máquina original: en la que se pueden obtener evidencias relativas a conexiones de red, datos volátiles en memoria y en general toda la información volátil del sistema.
- Análisis de una máquina virtual a partir de la copia de disco de la original: en la que podemos realizar las pruebas necesarias repetidas veces, una vez realizadas las copias correspondientes.

Herramientas por procesos

- Preparación

  La fase de preparación no es estrictamente una fase como tal. Como se ha explicado, se basa en disponer de todo lo necesario para afrontar el proyecto de investigación forense.

  Desarrollar los procesos de negocio, establecer los límite o alcance del proyecto, determinar los objetivos son tareas que, como se ha podido ver son perfectamente desarrollables utilizando Emacs como herramienta para la edición de textos.

  La herramienta necesaria para el desarrollo de los distintos procedimientos de documentación es Emacs, y adicionalmente el resto de herramientas que pueden utilizarse como Taskjuggler u similar.

- Identificación

  Para la fase de identificación se utilizarán las mismas herramientas que en el caso anterior, dado que como se ha explicado, hasta el proceso de recopilación no se inician tareas concretas diferentes del desarrollo de la base de conocimiento inicial.

  La herramienta necesaria para el desarrollo de los distintos procedimientos de documentación es Emacs, y adicionalmente el resto de herramientas que pueden utilizarse como Taskjuggler u similar.

- Recopilación

  Como ya se ha comentado es importante recolectar las evidencias en función de su mayor o menor volatilidad, por lo que en función de dicha prioridad, el orden propuesto es:

  ```
  - Registros de microprocesador.
  - Registros de dispositivos periféricos.
  - Información en cache.
  - Tabla de enrutamiento.
  - Tabla de cache de direcciones ARP.
  - Tabla de procesos.
  - Núcleo de estadísticas.
  - Información de memoria del sistema en ejecución.
  - Sistemas de archivos temporales.
  - Archivos almacenados en discos rígidos.
  - Datos de monitorización del sistema en ficheros de seguimiento.
  - Logs de procesos.
  - Configuración física.
  - Configuración de entorno.
  - Topología de red.
  - Medios de almacenamiento extraibles (CDs,DVDs, discos USB, etc).
  - Unidades de copia de seguridad.
  ```

  Sin embargo, es la experiencia del investigador y su percepción del entorno lo que tiene que determinar el orden de recogida.

  A continuación se desarrollan algunos de los procedimientos básicos a seguir dentro del proceso de recopilación, utilizando siempre herramientas de línea de comando que pueden ser lanzadas desde la shell de Emacs. No se va a desarrollar un caso por cada tipo de dato a recopilar ya que el número de casos de uso es muy alto.

- Copia de memoria

  Para realizar la copia de la memoria se utiliza el comando:

  ```
  dd if=/dev/mem of=memdump.img
  ```

  Con el contenido del fichero .img podemos utilizar comandos como `grep` para realizar búsquedas e identificar información interesante.

  En caso de realizar la copia a través de una red, podemos realizarlo utilizando el comando `netcat` para establecer una vía de comunicación con el objetivo.

  En el equipo analizado ejecutamos:

  ```
  dd if=/dev/mem | nc 192.168.1.5 4444
  ```

  y en el equipo remoto almacenamos el dump de memoria mediante el comando:

  ```
  nc -l -p 4444 > memdump.img
  ```

  where the ip address is the machine we want to send to and the second part (4444) is the port address. On the listening machine, we type 'nc -l -p 4444 >memdump.img' – here we are specifiying that we're listening locally (-l) and on port(-p) 4444.

- Hora del sistema

  La hora del sistema es un dato básico, ya que a la hora de desarrollar la cronología relacional o línea temporal un error en la misma puede dar lugar a conclusiones erróneas.

  Se obtiene mediante el comando `date` para CEST o `date -u` para UTC.

  ```
  bash-3.2$ date
  Tue Jun  9 13:23:54 CEST 2015
  bash-3.2$ date -u
  Tue Jun  9 11:24:01 UTC 2015
  bash-3.2$
  ```

- Borrado seguro de disco

  `Borrado seguro` o `disk wiping` es el proceso en el que se vuelcan datos de tipo 0 sobre un dispositivo seleccionado como destino, eliminando de este modo cualquier información anterior.

  El procedimiento de `borrado seguro` constituye un procedimiento indispensable para garantizar la higiene en el tratamiento y posterior análisis de las evidencias de cada caso. De esta forma, existe la certeza de que un disco contendrá información exclusiva de un caso, no quedando rastro de información alojada anteriormente en el dispositivo. Como hemos visto, esta circunstancia es especialmente importante ante la existencia en un disco de espacio supuestamente no utilizado.

  El proceso de `borrado seguro` no debe confundirse con el de `eliminación segura de información`, que trata de garantizar la no recuperación de la información que hubiese estado alojada en un dispositivo de almacenamiento.

  La `eliminación segura de información` requiere que se realicen varias pasadas de bits de unos (1) y ceros (0), asegurando de este modo que ninguna información será recuperable ni siquiera haciendo uso de elementos hardware altamente especializados. Sin embargo, en el caso del proceso de `disk wiping`, sólo es necesario realizar una pasada de bits a 1.

  Algunos ejemplos de comandos que permiten el `borrado seguro` son:

```
bash-3.2$ dd if=/dev/zero of=/dev/sda
bash-3.2$ dd if=/dev/urandom of=/dev/sda
bash-3.2$ dc3dd wipe=/dev/sda pat=random
bash-3.2$ dc3dd wipe=/dev/sda pat=110100100111
bash-3.2$ de3dd wipe=/dev/sda tpat=hello
```

- Adquisición de imágenes forenses

  Se ha comentado anteriormente que el equipamiento hardware es la opción más profesional e idónea para realizar los procesos de copiado necesarios, y es una afirmación correcta.

  Cuando un disco es clonado físicamente se duplica también el espacio no particionado. De este modo, ante la necesidad de recuperación de ficheros eliminados ésta puede efectuarse tanto en el espacio particionado como en aquel que no lo está. En este caso, aunque no es determinante, es importante que el dispositivo sobre el que se va a volcar la información tenga condiciones lógicas similares al de origen para evitar la aparición de problemas a la hora de arrancar el sistema operativo (sobretodo en análisis tipo Live Forensics) y reconocer el dispositivo de almacenamiento.

  Sin embargo, existen como alternativa, soluciones basadas en software que pueden encargarse de esta fase fundamental en todo análisis forense.

  La mayor parte de ellas hacen uso de la herramienta de copia `dd`, existente en entornos Unix y Linux, para la copia de un número determinado de bytes o de bloques.

  `dc3dd` es una modificación de la herramienta de copia bit a bit `dd`, que incluye ciertas características que facilitan la adquisición de imágenes forenses. Durante la ejecución de `dc3dd` el usuario puede ver información como el progreso de la cantidad de bytes copiados, el porcentaje del total, la cantidad de segundos incurridos, y la velocidad instantánea de copiado. Además, a medida que se realiza la imagen, también se calcula el hash del disco de origen en paralelo. Luego, una vez que termina el proceso de copiar los datos, se calcula el hash para la salida, y se contrasta contra el de origen.

  `dcfldd` también está basada en `dd`, pero se diferencia de `dc3dd` en que es una bifurcación de `dd`, no una actualización de la misma. Como consecuencia, `dcfldd` tiene similitudes con `dc3dd`, pero su código es distinto, y sus características también.

  Finalmente, `FTK Imager` facilita información de progreso adecuadamente, pero la característica fundamental que diferencia a esta herramienta de las otras dos comentadas anteriormente es la posibilidad de comprimir los archivos de salida.

  Como es lógico, la herramienta a elegir dependerá de las necesidades del investigador. En general, es recomendable utilizar `dc3dd` en lugar de `dcfldd` por la información provista y por la velocidad de copia. En los casos en que se desea almacenar varias imágenes de diversos activos en un mismo disco, o cuando sea necesario comprimir las imágenes por cuestiones de espacio, `FTK Imager` es la herramienta más adecuada.

- Hash - Integridad mediante firma digital de archivos

  Es recomendable modificar el algoritmo predeterminado de cálculo del hash, MD5. La utilización en su lugar de al menos SHA1 mejora sensiblemente el nivel de seguridad de la operación. Algunas de las motivaciones de esta modificación se recogen en el artículo del blog de Legalidad Informática.

  Queda por lo tanto que este modo garantizado que el investigador forense no ha realizado manipulación alguna de las pruebas desde el momento en que se realiza la adquisición de las mismas. Claro está que éste no puede extender esta garantía de no alteración con anterioridad a su intervención. No es inusual que los afectados o bien personal informático en

su representación, sí que hayan modificado las evidencias originales, de forma más o menos malintencionada dependiendo del caso. Sólo el posterior análisis dará respuesta a esta incertidumbre propia de toda investigación.

```
1  md5sum nombre_archivo
2  sha1sum nombre_archivo
3  sha256sum nombre_archivo
4  md5deep -e nombre_archivo
5  sha1deep nombre_archivo
6  sha256deep nombre_archivo
7  tigerdeep nombre_archivo
8  whirlpooldeep nombre_archivo
```

- Fuzzy Hashing

  Ssdeep y *sdhash* son dos algoritmos de fuzzy hashing que nos permite saber el nivel de similitud de dos o más archivos.

```
1  ssdeep -M nombre_archivo1 nombre_archivo2
```

- Preservación

  El proceso de preservación de las evidencias no contempla el uso de ninguna herramienta que no se haya comentado anteriormente.

- Análisis

  El proceso de análisis es el más heterogéneo a la hora de plantear el uso de herramientas para el análisis de las evidencias identificadas.

  Partiendo de conocimientos básicos como el sistema de ficheros (en el caso de unidades de almacenamiento) o sistema operativo (en el caso de dispositivos que dispongan de procesador) de las evidencias a analizar, tal como se explica en la metodología, se determinará un checklist de artefactos y de herramientas a utilizar.

  Muchos investigadores se plantean realizar exclusivamente el análisis del espacio particionado de la unidad de disco. Sin embargo el espacio no particionado puede contener información muy relevante, ya que la eliminación consciente de las particiones de un disco utilizando los procedimientos habitualmente no elimina la información que reside en el espacio no particionado.

  `File Carving` es una técnica de recuperación de ficheros basándose en la estructura de los ficheros y en el contenido, obviando las estructuras del sistema de ficheros.

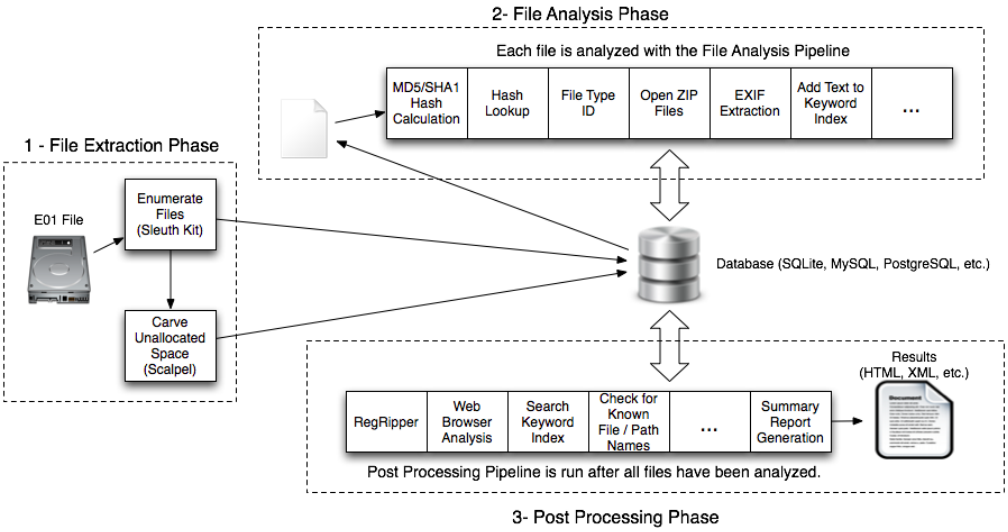
  Esta técnica es usada comúnmente para recuperar ficheros en el área de disco donde no hay nada almacenado desde el punto de vista de las estructuras del sistema de ficheros, lo que en el caso de dispositivos dañados equivale a considerar todo el espacio.

  Dado un dispositivo de almacenamiento, un File Carver podrá o no reconocer el sistema de ficheros usado, por lo que es tarea de este determinar que espacio está sin reservar. Esto en algunos casos significa que se trabajará sobre TODO el disco, lo que no es óptimo, por lo que para reducir esta cantidad de trabajo, las aplicaciones más avanzadas son capaces de identificar ficheros del sistema y ficheros pertenecientes a aplicaciones, todo esto basándose en Hashes MD5 y en palabras clave. Encase y Forensik Toolkit poseen esta funcionalidad que ahorrará mucho trabajo.

  Una de las herramientas que más me gusta a mi particularmente es bulk_extractor, sin embargo existen muchas otras herramientas que pueden ser útiles a la hora de recuperar ficheros como

`foremost`, `scalpel`, `magicrescue`, `photorec`, `recoverjpeg`, `extundelete`, `ntfsundelete` o `scrounge-ntfs` entre otras.

Por otro lado , una de los frameworks forenses más antiguos y actualmente más utilizados es sleuth-kit, que como se puede ver en el siguiente gráfico, consta de tres (3) fases de análisis desarrolladas por diferentes herramientas:



mac-robber es una herramienta de investigación digital que recoge datos de ficheros que se encuentran en sistemas de ficheros montados, lo que es muy útil durante el análisis de un sistema en vivo o para el análisis posterior de un sistema en un laboratorio.

Los datos pueden ser utilizados por la herramienta `mactime` de Sleuth Kit para hacer una línea de tiempo de actividad de los ficheros.

Inicialmente había conformado en este punto del proyecto una larga lista de herramientas de los distintos sistemas operativos que compartían la característica de ser ejecutables desde una shell y por lo tanto desde la shell de Emacs. Sin embargo al analizarla en detalle me he dado cuenta de que el listado no aportaba nada al objetivo del proyecto, por lo que decidí eliminarla. Es posible obtener herramientas adicionales de muchas fuentes libres disponibles en internet, y a continuación pongo varias de ellas:

- Proyecto Konfía
- Linux Forensics Tools Repository
- SIFT
- OS X Auditor: herramienta de análisis forense para Mac
- New version of Mac OS X Forensics Framework, Pac4Mac 0.3
- Nirsoft
- Sysinternals

- Consolidación

  La herramienta más importante para la consolidación de toda la información recabada es Emacs de nuevo, si se obvian herramientas básicas como el 'sentido común' y la 'objetividad'.

  Utilizando Emacs y siguiendo las buenas prácticas metodológicas relativas al desarrollo de los informes se consolidar toda la información obtenida durante la investigación y ésta, posteriormente,

puede ser facilitada en distintos formatos (ya que el formato ORG no es el más adecuado para directivos o personal no acostumbrado a trabajar con ficheros de texto plano) como HTML, PDF o similar.

Capítulo 8: PoC

La extensión del actual capítulo es importante y equivale al 50 % aproximadamente del documento. Esto se debe que a lo largo del documento se ha omitido el contenido de las plantillas y otra documentación desarrollada para el proyecto con el fin de que el volumen del mismo sea excesivo y se hace referencia a las carpetas donde ésta se puede consultar. Sin embargo, en la prueba de concepto, se ha considerado adecuado incorporar toda la documentación generada con el fin de tener un ejemplo práctico accesible y comentado, y evitar el tener que ir accediendo uno a uno a los distintos documentos facilitados en las carpetas.

```
Todos los documentos incorporados en la prueba de concepto aparecen con
el formato de texto con el que se escribe el actual párrafo para
facilitar su lectura o la omisión de la misma en función del interés del
lector.
```

Prueba de concepto

¿Porque un reto forense?
La respuesta es sencilla, si bien llegar a ella ha sido un proceso de prueba y error un tanto laborioso.
Inicialmente mi idea era plantear como prueba de concepto, siempre manteniendo Emacs como elemento central, un ejercicio globalmente amplio a nivel de entornos operativos de trabajo (Linux, MacOS y Windows), escenarios posibles (para realizar análisis live forensics, logical acquisition, sparse acquisition y post mortem) y plataformas analizadas (Linux, MacOS, Windows, iOS y Android) pero el mero planteamiento de un número mínimo de casos de uso a analizar hacía que el proyecto fuese inabarcable.
En segunda instancia traté de plantearlo manteniendo lo que entiendo que comprende todos los aspectos más importantes:

- Emacs como elemento principal.
- Seguir la metodología planteada fielmente.
- Maximizar los entornos de trabajo (Linux, MacOS y Windows).
- Maximizar el número de herramientas y pruebas a realizar.

Tras plantearme distintos alcances y descartarlos debido a que el coste en tiempo de desarrollo eran inasumibles observé que lo tenía que acotar era el escenario operativo y la plataforma a analizar, dado que las constantes que no podía obviar eran el uso de Emacs como elemento principal y la validación de la metodología planteada en función de los datos derivados de su uso.
En ese punto pensé que para comparar mi propuesta metodológica con algo realista, debería de poder comparar mis resultados con los de otras personas y, de este modo, recordé los retos forenses de Red Iris que conocí hace años.
Analizando varios retos, seleccioné el Reto Forense - Episodio III ya que a diferencia del resto conseguí disponer de todos los elementos que necesitaba:

- Los binarios a analizar.
- Los informes desarrollados por los participantes.

En este caso el reto forense se trata en el capítulo actual desde una perspectiva de investigación forense, presuponiendo una solicitud por parte de un supuesto cliente, que tiene la intención de ir a juicio en el caso de que se identifique una intrusión y al autor de la misma. Por lo tanto, el uso de una metodología y medios adecuados así como el cumplimiento de la legislación española son críticos a la hora de presentar el informe forense, que es el objetivo final del reto planteado.

Entorno de trabajo: Estación forense

En un primer momento se plantean las tres alternativas lógicas a la hora de seleccionar la plataforma operativa para soportar la estación de trabajo forense:

- Linux
- MacOS
- Windows

La primera premisa, que cumple cada una de las plataformas, es la posibilidad de instalar y utilizar Emacs y la totalidad de la funcionalidad del mismo requerido por el desarrollo de la metodología planteada en el PFC.
Además, cada una de las plataformas operativas es perfectamente funcional y dispone de herramientas forenses adecuadas para realizar las distintas labores forenses de forma alineada con los requisitos metodológicos y legales que son requeridos.
Hasta este punto cualquiera de las alternativas es viable, sin embargo, se ha descartado como estación de trabajo forense la plataforma operativa:

- Windows: por los problemas derivados del licenciamiento del sistema operativo a medio plazo.
- MacOS: por la complejidad a la hora de virtualizar la plataforma operativa.

Por lo tanto, como es obvio, se ha seleccionado la plataforma operativa Linux como estación de trabajo forense. Pero ¿cual de los distintos sabores de Linux es el más adecuado?
En mi caso seleccionaría Linux Debian dado que se trata de mi plataforma de uso diaria, sin embargo, otra alternativa que surge inmediatamente al plantear esta cuestión es el uso de una de las varias distribuciones forenses actualmente presentes y en continua evolución.
Tras analizar las alternativas la decisión ha sido un planteamiento mixto. He seleccionado la distribución mini de Ubuntu 64bits sobre la que es posible desplegar el entorno forense de SIFT, LXDE como entorno de escritorio X11 liviano, Emacs y cualquier otra herramienta que se requiera.
En el contexto descrito se ha instalado una máquina virtual con los siguientes paquetes:

- ENTORNO Linux
  - ☒ VM SIFT (Sans Forensics)
    - `http://sift.readthedocs.org/en/latest/packages/index.html#all-packages`
    - sleuthkit/Autopsy
    - mac-robber
    - mactime
    - dcfldd
    - dc3dd
    - tcpdump
    - wireshark
    - Plaso
    - bulk_extractor
      - `http://www.dragonjar.org/data-carvers-en-retos-forenses.xhtml`
      - `http://www.dragonjar.org/bulk-extractor.xhtml`
    - libqcow-tools

    - libsmdev-tools
    - libsmraw-tools
    - libvhdi-tools
    - libvmdk-tools
- ☒ Emacs 24
- ☒ tmux
- ☒ parcellite/glipper/klipper/
- ☒ sshfs
- ☒ autofs
- ☒ memdump
- ☒ lime forensics

Se ha creado el siguiente usuario:

- Usuario: investigador
- Contraseña: forense

Se ha generado el par de claves para el usuario `Investigador Forense`, con dirección de correo inventada `investigador@forense.fi.upm.es`:

```
investigador@EFI:~$ gpg --edit-key 29678D06
gpg (GnuPG) 1.4.16; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Clave secreta disponible.

pub  2048R/29678D06  creado: 2015-05-26  [caduca: nunca     ]  uso: SC
                     confianza: absoluta      validez: absoluta
sub  2048R/DAC61BAB  creado: 2015-05-26  [caduca: nunca     ]  uso: E
[  absoluta ] (1). Investigador Forense (Cifrado de información crítica
de proyectos forenses digitales) <investigador@forense.fi.upm.es>
```

Reto forense UNAM Episodio III

Para el desarrollo de la labor de investigación del reto forense se ha seguido la metodología DIEM propuesta en el actual proyecto.
Los ficheros desarrollados se pueden consultar en el directorio de trabajo creado siguiendo la metodología.

Bitácora (Registro de acciones realizadas)

Inicialmente se trabaja sobre buffers de Emacs (sin ficheros asociados) y, una vez se han creado los directorios de proyecto, se almacenan en disco.

```
#+TITLE: Registro de acciones realizadas
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:2 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='./DOC_ANEXA/work.css' />

#+BEGIN: clocktable :maxlevel 2 :scope file
#+CAPTION: Clock summary at [2015-06-21 Sun 21:53]
| Headline                                    |       Time |          |
|---------------------------------------------+------------+----------|
| *Total time*                                | *5d 17:56* |          |
|---------------------------------------------+------------+----------|
| Proceso de Preparación                      |      18:03 |          |
| \emsp Registro de acciones...               |            |     0:05 |
| \emsp Plan de proyecto                      |            |    13:38 |
| \emsp Estructura de directorios             |            |     0:11 |
| \emsp Acuerdo de confidencialidad           |            |     0:21 |
| \emsp Antecedentes                          |            |     0:32 |
| \emsp Fichero de datos generales            |            |     0:23 |
| \emsp Autorización y aceptación de trabajos |            |     0:18 |
| \emsp Registro de limitaciones y exclusiones|            |     1:11 |
| \emsp Documento de inicio de proyecto       |            |     1:24 |
| Proceso de identificación                   |       3:53 |          |
| \emsp Registro de incidencias               |            |     0:11 |
| \emsp Identificación de palabras clave      |            |     0:13 |
| \emsp Identificación de actores y cuadro... |            |     1:50 |
| \emsp Croquis del escenario                 |            |     1:25 |
| \emsp Identificación de activos involucrados|            |     0:14 |
| Proceso de recopilación (recolección...     |       0:55 |          |
| \emsp Cadena de custodia                    |            |     0:55 |
| Proceso de preservación                     |       0:15 |          |
| \emsp Tiempo dedicado a la preservación de... |          |     0:15 |
| Proceso de análisis                         |    3d 8:11 |          |
| \emsp Checklist de herramientas HW/SW       |            |     6:22 |
| \emsp Checklist de artefactos               |            |     2:58 |
| \emsp Análisis de datos y evidencias        |            | 2d 16:57 |
| \emsp Cronología relacional o línea temporal|            |     5:54 |
| Proceso de consolidación                    |   1d 10:39 |          |
| \emsp Informe técnico                       |            | 1d 10:08 |
```

```
| \emsp Documento de aceptación de fin de...    |            |     0:31 |
#+END:

* Proceso de Preparación   :Finalizado:
** Registro de acciones realizadas(Bitácora)  :Finalizado:
  CLOCK: [2015-05-26 Tue 23:58]--[2015-05-27 Wed 00:03] =>  0:05

- Se inicia el buffer correspondiente al registro de acciones
  realizadas.
- El resto de entradas en la bitácora imputarán el tiempo dentro de sus
  correspondientes tareas.

** Plan de proyecto  :Finalizado:
  CLOCK: [2015-05-27 Wed 15:31]--[2015-05-27 Wed 22:03] =>  6:32
  CLOCK: [2015-05-27 Wed 07:35]--[2015-05-27 Wed 14:15] =>  6:40
  CLOCK: [2015-05-27 Wed 00:15]--[2015-05-27 Wed 00:37] =>  0:22
  CLOCK: [2015-05-27 Wed 00:04]--[2015-05-27 Wed 00:08] =>  0:04

- Se inicia el desarrollo del Plan de proyecto.
- Se desarrolla el fichero principal de proyecto de TaskJuggler basado
  en el utilizado para plantear el proyecto.
- Se desarrolla el  [[../1_PLANIFICACION/10-PoC.tji][fichero a importar]]
  desde el fichero principal que
  contiene las especificaciones concretas de la investigación a
  realizar.
- En este caso se va a actualizar el fichero anterior en función de los
  datos recolectados en el fichero de bitácora para realizar el
  seguimiento y cumplimiento del proyecto. Se ha creado un
  [[../1_PLANIFICACION/20-jljerez.tji][segundo
  fichero a importar]] cuyo cometido es controlar el tiempo dedicado a las
  tareas de forma detallada (o booking) pero ya lo hacemos con el
  anterior registro. La [[http://www.emacswiki.org/emacs/Taskjuggler]
  [integración de Emacs y Taskjuggler]] no es
  estable, por lo que se ha optado por no utilizar el modo menor
  ~taskjuggler-mode~ como parte del proyecto. Este segundo fichero se
  presenta sin contenido.
- El resto de tiempo asociado a esta tarea relativo a la actualización
  del fichero de tareas imputarán el tiempo dedicado dentro de sus
  correspondientes tareas.

** Estructura de directorios  :Finalizado:
  CLOCK: [2015-05-28 Thu 00:04]--[2015-05-28 Thu 00:15] =>  0:11

- Se crea la estructura de directorios establecida por la metodología
  sobre el directorio de proyecto ~PoC-PFC-001~.

** Acuerdo de confidencialidad  :Finalizado:
   CLOCK: [2015-05-28 Thu 19:34]--[2015-05-28 Thu 19:55] =>  0:21
```

- Se crea una primera versión del [[~/pfc/PFC%20-%20PoC-PFC-001/0_INF_BASE
  /PoC_Datos_generales.org][fichero de datos generales
  PoC_Datos_generales.org]] y, utilizando la función Emacs Lisp
  [[../../DOC_ANEXA/pfc.el][gpgFilesToPDF]] desarrollada para el actual PFC,
  conjuntamente con el
  fichero de datos y la plantilla del
  [[../../PLANTILLAS/Acuerdo%20de%20confidencialidad.org]
  [acuerdo de confidencialidad]] se crea
  el [[./PoC-AC-001.org.pdf][acuerdo de confidencialidad PoC-AC-001.org.pdf]].

** Antecedentes :Finalizado:
  CLOCK: [2015-05-29 Fri 23:30]--[2015-05-29 Fri 23:36] => 0:05
  CLOCK: [2015-05-28 Thu 21:14]--[2015-05-28 Thu 21:40] => 0:26

- Se crea el fichero ORG de antecedentes. En teoría se desarrollaría a
  lo largo de una reunión con el cliente. Sin embargo, en este caso no
  existe tal opción, por lo que se obtienen los antecedentes de las
  explicaciones de la página web del reto forense
  http://www.seguridad.unam.mx/eventos/reto/.

- Creación del fichero [[./PoC-ATC-001.org.pdf][pdf de antecedentes]].

** Fichero de datos generales :Finalizado:
  CLOCK: [2015-05-29 Fri 23:35]--[2015-05-29 Fri 23:58] => 0:23

- Se genera el fichero [[./PoC_Datos_generales.org][de datos generales]].

** Autorización y aceptación de trabajos :Finalizado:
  CLOCK: [2015-05-30 Sat 07:52]--[2015-05-30 Sat 08:10] => 0:18

Creación del documento [[./PoC-AAT-001.org.pdf][Autorización y aceptación de trabajos]].

** Registro de limitaciones y exclusiones :Finalizado:
  CLOCK: [2015-06-04 Thu 01:14]--[2015-06-04 Thu 02:25] => 1:11

- Creación del [[./PoC-PFC-001/0_INF_BASE/PoC-RE-001.org]
  [registro de exclusiones]] inicial.
** Documento de inicio de proyecto :Finalizado:
  CLOCK: [2015-06-06 Sat 10:03]--[2015-06-06 Sat 10:38] => 0:35
  CLOCK: [2015-06-05 Fri 20:56]--[2015-06-05 Fri 21:45] => 0:49

- Se crea el documento de [[./PoC-DIP-001.org.pdf][inicio de proyecto]].
* Proceso de identificación :Finalizado:
** Registro de incidencias :Finalizado:
   CLOCK: [2015-06-12 Fri 10:21]--[2015-06-12 Fri 10:32] => 0:11

- Se crea el documento sin contenido.

** Identificación de palabras clave :Finalizado:
  CLOCK: [2015-06-06 Sat 12:04]--[2015-06-06 Sat 12:17] => 0:13

- Se inicia el documento con los datos básicos.

** Identificación de actores y cuadro relacional :Finalizado:
   CLOCK: [2015-06-12 Fri 17:11]--[2015-06-12 Fri 18:55] => 1:44
   CLOCK: [2015-06-12 Fri 17:05]--[2015-06-12 Fri 17:11] => 0:06

- Se crea el documento de identificación de actores.
- Se crea el cuadro relacional basado en Graphviz.
  + Se ha requerido de más tiempo debido a que no se tenía instalado el
    entorno graphviz.

** Croquis del escenario :Finalizado:
   CLOCK: [2015-06-13 Sat 11:53]--[2015-06-13 Sat 12:25] => 0:32
   CLOCK: [2015-06-13 Sat 11:13]--[2015-06-13 Sat 11:28] => 0:15
   CLOCK: [2015-06-13 Sat 10:33]--[2015-06-13 Sat 11:11] => 0:38

- Se identifican todos los indicios que hay en el escenario.
- Se realiza un documento fotográfico.
  + Se ha realizado un ejercicio imaginativo para este documento.
- Se realiza un croquis del escenario.
  + Se ha utilizado la herramienta ~ditaa~ para el croquis.

** Identificación de activos involucrados :Finalizado:
   CLOCK: [2015-06-13 Sat 17:32]--[2015-06-13 Sat 17:46] => 0:14

- Se realiza el cuadro de identificación de activos involucrados.

* Proceso de recopilación (recolección o adquisición) :Finalizado:
** Cadena de custodia :Finalizado:
   CLOCK: [2015-06-14 Sun 10:59]--[2015-06-14 Sun 11:54] => 0:55

- Se inicia la documentación de la cadena de custodia de las diferentes
  evidencias.

* Proceso de preservación :Finalizado:
** Tiempo dedicado a la preservación de las evidencias :Finalizado:
   CLOCK: [2015-06-14 Sun 13:55]--[2015-06-14 Sun 14:10] => 0:15

- Se verifica la correcta preservación de las evidencias en función de
  la metodología propuesta.

* Proceso de análisis   :Finalizado:
** Checklist de herramientas HW/SW :Finalizado:
   CLOCK: [2015-06-15 Mon 15:20]--[2015-06-15 Mon 20:19] => 4:59
   CLOCK: [2015-06-15 Mon 13:04]--[2015-06-15 Mon 14:27] => 1:23

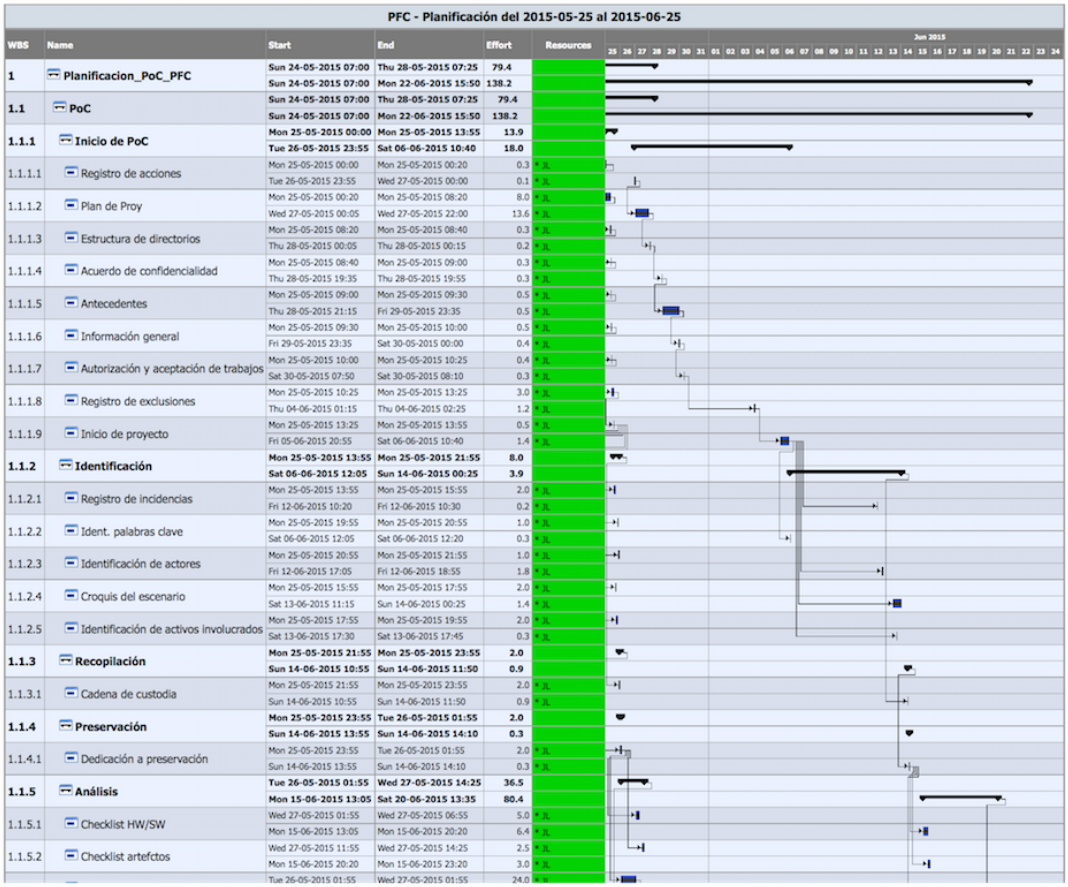
```
- Se inicia el desarrollo del checklist de herramientas adecuadas a la
  investigación, independientemente de que al final se utilicen o no.
- Se complementa el documento.

** Checklist de artefactos  :Finalizado:
   CLOCK: [2015-06-15 Mon 20:21]--[2015-06-15 Mon 23:19] =>  2:58

- Se inicia el desarrollo del checklist de herramientas adecuadas a la
  investigación, independientemente de que al final se utilicen o no.

** Análisis de datos y evidencias  :Finalizado:
   CLOCK: [2015-06-19 Fri 17:07]--[2015-06-20 Sat 01:40] =>  8:33
   CLOCK: [2015-06-19 Fri 07:54]--[2015-06-19 Fri 15:07] =>  7:13
   CLOCK: [2015-06-18 Thu 14:27]--[2015-06-19 Fri 02:29] => 12:02
   CLOCK: [2015-06-18 Thu 08:02]--[2015-06-18 Thu 13:45] =>  5:43
   CLOCK: [2015-06-17 Wed 14:03]--[2015-06-18 Thu 01:13] => 11:10
   CLOCK: [2015-06-17 Wed 09:38]--[2015-06-17 Wed 13:03] =>  3:25
   CLOCK: [2015-06-16 Tue 22:00]--[2015-06-17 Wed 02:02] =>  4:02
   CLOCK: [2015-06-16 Tue 14:33]--[2015-06-16 Tue 21:00] =>  6:27
   CLOCK: [2015-06-16 Tue 07:37]--[2015-06-16 Tue 13:59] =>  6:22
   :PROPERTIES:
   :ORDERED:  t
   :END:

,- Se inicia el análisis.

** Cronología relacional o línea temporal  :Finalizado:
   CLOCK: [2015-06-20 Sat 07:41]--[2015-06-20 Sat 13:35] =>  5:54

- Se inicia el documento de línea temporal.

* Proceso de consolidación  :Finalizado:
** Informe técnico  :Finalizado:
   CLOCK: [2015-06-22 Mon 07:51]--[2015-06-22 Mon 14:20] =>  6:29
   CLOCK: [2015-06-21 Sun 15:30]--[2015-06-22 Mon 01:50] => 10:20
   CLOCK: [2015-06-21 Sun 07:46]--[2015-06-21 Sun 13:33] =>  5:49
   CLOCK: [2015-06-20 Sat 14:10]--[2015-06-21 Sun 01:42] => 11:32

- Se inicia el informe técnico.

** Documento de aceptación de fin de proyecto  :Finalizado:
   CLOCK: [2015-06-22 Mon 15:23]--[2015-06-22 Mon 15:54] =>  0:31

- Se inicia el documento de aceptación de fin de proyecto.
```

El fichero puede ser accedido mediante el enlace `./PoC-PFC-001/0_INF_BASE/PoC-RAR-001.org`

Plan de proyecto

Se ha desarrollado con Taskjuggler una planificación previa con las tareas a desarrollar y la estimación del tiempo (`plan`) que cree que se va a dedicar a cada una de ellas.
El documento principal desarrollado, donde se especifican los parámetros generalistas del proyecto, en principio no se ha acotado el horario de trabajo, pudiendo dedicar las 24 horas del día incluso en fin de semana y festivos al desarrollo de la investigación. Se ha tomado esta decisión ya que los datos que se van a tomar son los reales, las horas concretas sobre las que voy a trabajar en las tareas que se describen, y no voy a limitar las horas de trabajo.
Por lo demás, se han desarrollado dos informes:

- Diagrama de Gantt: proyecto en html
- Diagrama de recursos: uso de recursos en html



WBS	Name	Start	End	Effort	Resources
1	Planificacion_PoC_PFC	Sun 24-05-2015 07:00	Thu 28-05-2015 07:25	79.4	
		Sun 24-05-2015 07:00	Mon 22-06-2015 15:50	138.2	
1.1	PoC	Sun 24-05-2015 07:00	Thu 28-05-2015 07:25	79.4	
		Sun 24-05-2015 07:00	Mon 22-06-2015 15:50	138.2	
1.1.1	Inicio de PoC	Mon 25-05-2015 00:00	Mon 25-05-2015 13:55	13.9	
		Tue 26-05-2015 23:55	Sat 06-06-2015 10:40	18.0	
1.1.1.1	Registro de acciones	Mon 25-05-2015 00:00	Mon 25-05-2015 00:20	0.3	JL
		Tue 26-05-2015 23:55	Wed 27-05-2015 00:00	0.1	JL
1.1.1.2	Plan de Proy	Mon 25-05-2015 00:20	Mon 25-05-2015 08:20	8.0	JL
		Wed 27-05-2015 00:05	Wed 27-05-2015 22:00	13.6	JL
1.1.1.3	Estructura de directorios	Mon 25-05-2015 08:20	Mon 25-05-2015 08:40	0.3	JL
		Thu 28-05-2015 00:05	Thu 28-05-2015 00:15	0.2	JL
1.1.1.4	Acuerdo de confidencialidad	Mon 25-05-2015 08:40	Mon 25-05-2015 09:00	0.3	JL
		Thu 28-05-2015 19:35	Thu 28-05-2015 19:55	0.3	JL
1.1.1.5	Antecedentes	Mon 25-05-2015 09:00	Mon 25-05-2015 09:30	0.5	JL
		Thu 28-05-2015 21:15	Fri 29-05-2015 23:35	0.5	JL
1.1.1.6	Información general	Mon 25-05-2015 09:30	Mon 25-05-2015 10:00	0.5	JL
		Fri 29-05-2015 23:35	Sat 30-05-2015 00:00	0.4	JL
1.1.1.7	Autorización y aceptación de trabajos	Mon 25-05-2015 10:00	Mon 25-05-2015 10:25	0.4	JL
		Sat 30-05-2015 07:50	Sat 30-05-2015 08:10	0.3	JL
1.1.1.8	Registro de exclusiones	Mon 25-05-2015 10:25	Mon 25-05-2015 13:25	3.0	JL
		Thu 04-06-2015 01:15	Thu 04-06-2015 02:25	1.2	JL
1.1.1.9	Inicio de proyecto	Mon 25-05-2015 13:25	Mon 25-05-2015 13:55	0.5	JL
		Fri 05-06-2015 20:55	Sat 06-06-2015 10:40	1.4	JL
1.1.2	Identificación	Mon 25-05-2015 13:55	Mon 25-05-2015 21:55	8.0	
		Sat 06-06-2015 12:05	Sun 14-06-2015 00:25	3.9	
1.1.2.1	Registro de incidencias	Mon 25-05-2015 13:55	Mon 25-05-2015 15:55	2.0	JL
		Fri 12-06-2015 10:20	Fri 12-06-2015 10:30	0.2	JL
1.1.2.2	Ident. palabras clave	Mon 25-05-2015 19:55	Mon 25-05-2015 20:55	1.0	JL
		Sat 06-06-2015 12:05	Sat 06-06-2015 12:20	0.3	JL
1.1.2.3	Identificación de actores	Mon 25-05-2015 20:55	Mon 25-05-2015 21:55	1.0	JL
		Fri 12-06-2015 17:05	Fri 12-06-2015 18:55	1.8	JL
1.1.2.4	Croquis del escenario	Mon 25-05-2015 15:55	Mon 25-05-2015 17:55	2.0	JL
		Sat 13-06-2015 11:15	Sun 14-06-2015 00:25	1.4	JL
1.1.2.5	Identificación de activos involucrados	Mon 25-05-2015 17:55	Mon 25-05-2015 19:55	2.0	JL
		Sat 13-06-2015 17:30	Sat 13-06-2015 17:45	0.3	JL
1.1.3	Recopilación	Mon 25-05-2015 21:55	Mon 25-05-2015 23:55	2.0	
		Sun 14-06-2015 10:55	Sun 14-06-2015 11:50	0.9	
1.1.3.1	Cadena de custodia	Mon 25-05-2015 21:55	Mon 25-05-2015 23:55	2.0	JL
		Sun 14-06-2015 10:55	Sun 14-06-2015 11:50	0.9	JL
1.1.4	Preservación	Mon 25-05-2015 23:55	Tue 26-05-2015 01:55	2.0	
		Sun 14-06-2015 13:55	Sun 14-06-2015 14:10	0.3	
1.1.4.1	Dedicación a preservación	Mon 25-05-2015 23:55	Tue 26-05-2015 01:55	2.0	JL
		Sun 14-06-2015 13:55	Sun 14-06-2015 14:10	0.3	JL
1.1.5	Análisis	Tue 26-05-2015 01:55	Wed 27-05-2015 14:25	36.5	
		Mon 15-06-2015 13:05	Sat 20-06-2015 13:35	80.4	
1.1.5.1	Checklist HW/SW	Wed 27-05-2015 01:55	Wed 27-05-2015 06:55	5.0	JL
		Mon 15-06-2015 13:05	Mon 15-06-2015 20:20	6.4	JL
1.1.5.2	Checklist artefctos	Wed 27-05-2015 11:55	Wed 27-05-2015 14:25	2.5	JL
		Mon 15-06-2015 20:20	Mon 15-06-2015 23:20	3.0	JL
		Tue 26-05-2015 01:55	Wed 27-05-2015 01:55	24.0	JL

Adicionalmente se han desarrollado dos documentos que se incluyen en el principal durante la compilación del mismo y que especifican los datos concretos relativos a las tareas (10-PoC.tji) y los datos relativos a las horas invertidas, conocido como ~ booking, de cada recurso (20-jljerez.tji).

```
investigador@EFI:~$ tj3 00-Planificacion_PoC_PFC.tjp
TaskJuggler v3.5.0 - A Project Management Software

Copyright (c) 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013
              by Chris Schlaeger <chris@linux.com>

This program is free software; you can redistribute it and/or modify it under
```

```
the terms of version 2 of the GNU General Public License as published by the
Free Software Foundation.

Reading file 00-Planificacion_PoC_PFC.tjp                    [      Done      ]
Preparing scenario Plan                                      [      Done      ]
Scheduling scenario Plan                                     [      Done      ]
Checking scenario Plan                                       [      Done      ]
Preparing scenario Actual                                    [      Done      ]
Scheduling scenario Actual                                   [      Done      ]
Checking scenario Actual                                     [      Done      ]
Report 00-PFC-plan=2015-05-25=2015-06-25                     [      Done      ]
Report 40-jljerez-actual=2015-05-25=2015-06-25               [      Done      ]
```

Cada uno de los documentos puede verse en detalle a continuación:

```
project codProy 'PFC-JLJ'  2015-05-24-0:00--0500 +6m {

timingresolution 5min

# Hide the clock time. Only show the date.
timezone 'Europe/Madrid'
timeformat '%d-%m-%Y'
dailyworkinghours 8

# The currency for all money values is EUR.

currency 'EUR'

weekstartsmonday

# de lunes a jueves se viernes 4 horas diarias

workinghours mon - fri 00:00 - 23:59

  # fines de semana 5 horas diarias

workinghours sat, sun 00:00 - 23:59

  scenario plan 'Plan' {
    scenario actual 'Actual'
scenario test 'Test Scenario' {
      active no
    }
  }

extend resource {
    text Phone 'Phone'
}

  trackingscenario actual
```

```
  now 2015-07-20-11:00

}

shift jornada_verano 'Horario de la jornada de verano' {
  # Special working hours Monday to Wednesday. Use program defaults
  # for other days.
  workinghours mon - fri 8:00 - 13:00, 14:00 - 20:00
  workinghours sat, sun 9:00 - 12:00, 16:00 - 20:00
}

flags rolledup

# The daily default rate of all resources. This can be overriden for each
# resource. We specify this, so that we can do a good calculation of
# the costs of the project.

#-----------------------------------------------------------------------------#
#                                Calendarios                                  #
#-----------------------------------------------------------------------------#

# Calendario laboral Madrid 2015
vacation 'Reyes' 2015-01-07
vacation 'San José' 2015-03-18
vacation 'Jueves Santo' 2015-03-28
vacation 'Viernes Santo' 2015-03-29
vacation 'Trabajo' 2015-05-01
vacation 'Comunidad de Madrid'' 2015-05-02
vacation 'San Isidro' 2015-05-15
vacation 'Asunción de la Virgen' 2015-08-15
vacation 'Hispanidad' 2015-10-12
vacation 'Todos los santos' 2015-11-01
vacation 'La Almudena' 2015-11-09
vacation 'Constitución 2015-12-06
vacation 'Inmaculada Concepción' 2015-12-08
vacation 'Navidad' 2015-12-25

#-----------------------------------------------------------------------------#
#                                  Recursos                                   #
#-----------------------------------------------------------------------------#


resource jljerez 'JL' {
  efficiency 1
  email 'jljerez@error0x01.net'
  Phone '+34 650 66 99 15'
  rate 480
}
```

```
#-----------------------------------------------------------------------------#
#                                    Macros                                   #
#-----------------------------------------------------------------------------#

# Macro to set the background color of a cell according to the alert
# level of the task.

macro AlertColor [
  cellcolor plan.alert = 0 '#00D000' # green
  cellcolor plan.alert = 1 '#D0D000' # yellow
  cellcolor plan.alert = 2 '#D00000' # red
]

macro planificacion_PFC_periodo [
  taskreport '00-PFC-plan=${1}=${2}' {
    headline 'PFC - Planificación del ${1} al ${2}'
    scenarios plan, actual
    formats html
    period ${1} - ${2}
    sorttasks tree
    # hidetask ~isongoing(actual)
    columns bsi { title 'WBS' }, name, start, end, effort, resources { width 100 ${AlertColor}
            listtype bullets
            listitem '<-query attribute='name'->'
            start ${projectstart} end ${projectend}}, chart { scale day width 1500 }
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit hours
  }
]

macro asignacion_recurso [
  resourcereport '40-${1}-actual=${3}=${4}' {
    headline '${2} - Planificación del ${3} al ${4}'
    scenarios actual
    formats html
    period ${3} - ${4}
    hidetask ~(isdutyof(${1}, actual) & isactive(actual))
    hideresource ~(actual.id = '${1}')
    columns no, name { width 300 }, start, end, effort, effortdone, chart { scale day width 1024
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit hours
    numberformat '-' '' '' '.' 2
  }
]

macro planificacion_tarea [
  taskreport 'IF-${1}' {
    headline '${2} - Planificación completa'
```

```
    scenarios actual
    formats html
    hidetask ~(plan.id = '${1}' | ischildof(${1}))
    columns no, name, start, end, effort, chart { scale day width 1024 }
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit hours
  }
]

macro planificacion_tarea_periodo [
  taskreport 'IF-${1}=${3}=${4}' {
    headline '${2} - Planificación del ${3} al ${4}'
    scenarios actual
    formats html
    period ${3} - ${4}
    hideresource 0
    hidetask ~(actual.id = '${1}' | (ischildof(${1}) & isongoing(actual)))
    columns no, name { width 300 }, start, end, effort, chart { scale day width 1024 }
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit hours
  }
]

macro planificacion_ejecutiva_periodo [
  taskreport 'IE-${1}=${3}=${4}' {
    headline '${2} - Planificación del ${3} al ${4} / <-query attribute='now'-> '
    scenarios plan, actual
    formats html
    period ${3} - ${4}
    hidetask ~(actual.id = '${1}' | (ischildof(${1}) & isongoing(actual)))
    columns no, name { width 300 }, start, end, effort, chart { scale week width 1024 }
    timeformat '%a %d-%m-%Y %H:%M'
    rolluptask ((treelevel() > 2) | rolledup)
    loadunit hours
  }
]

macro planificacion_externa_tarea_periodo [
  taskreport 'IFE-${1}=${3}=${4}' {
    headline '${2} - Planificación del ${3} al ${4}'
    scenarios actual
    formats html
    period ${3} - ${4}
    hidetask ~(plan.id = '${1}' | ischildof(${1}))
    hideresource 1
    columns no, name, start, end, effort, chart { scale day width 1024 }
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit days
  }
```

```
]

macro horas_recurso [
  resourcereport 'HR-RI-${1}=${3}=${4}' {
    headline '${2} - Dedicación del ${3} al ${4}'
    scenarios actual
    formats html
    period ${3} - ${4}
    hidetask ~(isdutyof(${1}, actual) & isactive(actual))
    hideresource ~(actual.id = '${1}')
    columns no, name { width 300 }, start, end, effort, effortdone, daily { scale day width 1024
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit hours
  }
]

macro planificacion_recurso [
  resourcereport 'IP-RI-${1}=${3}=${4}' {
    headline '${2} - Planificación del ${3} al ${4}'
    scenarios plan
    formats html
    period ${3} - ${4}
    hidetask ~(isdutyof(${1}, plan) & isactive(plan))
    hideresource ~(plan.id = '${1}')
    columns no, name, start, end, effortdone, chart { scale day width 1024 }
    timeformat '%a %d-%m-%Y %H:%M'
    loadunit hours
  }
]

#-------------------------------------------------------------------------------#
#                              Proyecto                                         #
#-------------------------------------------------------------------------------#

task pfc_PoC 'Planificacion_PoC_PFC' { }
include '10-PoC.tji' { }

#-------------------------------------------------------------------------------#
#                              Asignaciones                                     #
#-------------------------------------------------------------------------------#

include '20-jljerez.tji' { }

#-------------------------------------------------------------------------------#
#                                  Informes                                     #
#-------------------------------------------------------------------------------#

${planificacion_PFC_periodo '2015-05-25' '2015-06-25'}
${asignacion_recurso 'jljerez' 'Jose Luis Jerez' '2015-05-25' '2015-06-25'}
```

```
# NOTA: El formato de fecha es YYYY-MM-DD.
# NOTA: Establecer dependencias (Ej. depends !!ini1.ini13)

supplement task pfc_PoC {

    task poc 'PoC' {

          start ${projectstart}

         # Tareas iniciales del proyecto
         task ini 'Inicio de PoC' {

              allocate jljerez {mandatory}
        priority 1000
        plan:start 2015-05-25
              actual:start 2015-05-27

              # Registro de acciones realizadas (Bitácora de investigación)
        # Solo se considera el tiempo de creación del documento
        # Los tiempos restantes se aplican a las tareas realizadas
        # como parte de la tarea global de documentación
               task RegAcc 'Registro de acciones' {
                    plan:effort 20min
                    actual:effort 5min
           complete 100
               }

               # Creación del Plan de Proyecto con Taskjuggler
          # y el tiempo dedicado a actualizarlo se aplica
          # como parte de la tarea global de documentación
               task planP 'Plan de Proy' {
            depends !RegAcc
         plan:effort 8.0h
         actual:effort 815min
         complete 100
               }

               # Creación de la estructura de directorios de la investigación.
               task EstrDir 'Estructura de directorios' {
            depends !planP
         plan:effort 20min
         actual:effort 10min
         complete 100
               }

               # Acuerdo de confidencialidad.
               task AcuConf 'Acuerdo de confidencialidad' {
         depends !EstrDir
         plan:effort 20min
```

```
 actual:effort 20min
 complete 100
       }

       # Documentación: antecedentes de la investigación.
       task Ant 'Antecedentes' {
 depends !AcuConf
 plan:effort 0.5h
 actual:effort 30min
 complete 100
       }

       # Documentación: información general de la investigación.
       task InfGen 'Información general'' {
 depends !Ant
 plan:effort 0.5h
 actual:effort 25min
 complete 100
}

       # Firma del documento de autorización y aceptación de trabajos.
       task Aut 'Autorización y aceptación de trabajos' {
 depends !InfGen
 plan:effort 25min
 actual:effort 20min
 complete 100
       }

# Documentación: Registro de exclusiones (Legales y Políticas del
      # cliente)
       task RegExc 'Registro de exclusiones' {
 depends !Aut
 plan:effort 3.0h
 actual:effort 70min
 complete 100
       }

       # Documentación: Documento de inicio de proyecto.
       task IniPro 'Inicio de proyecto' {
 depends !RegExc
 plan:effort 0.5h
 actual:effort 85min
 complete 100
       }
 }

 # En este punto se arrancan las tareas de identificación
 task idn 'Identificación' {
```

```
allocate jljerez {mandatory}
priority 1000

          # Registro de incidencias.
          task regInc 'Registro de incidencias' {
               plan:effort 2.0h
               actual:effort 10min
   complete 100
   depends !!ini.IniPro
          }

          # Identificación de palabras clave.
          task idPaCl 'Ident. palabras clave' {
               plan:effort 1.0h
               actual:effort 15min
   complete 100
   depends !!ini.IniPro
          }

          # Identificación de actores.
          task idAc 'Identificación de actores' {
               plan:effort 1.0h
               actual:effort 110min
   complete 100
   depends !!ini.IniPro
          }

          # Croquis del escenario.
          task crEs 'Croquis del escenario' {
               plan:effort 2.0h
               actual:effort 85min
   complete 100
   depends !!ini.IniPro
          }

          # Identificación de activos involucrados
          task idAI 'Identificación de activos involucrados' {
               plan:effort 2.0h
               actual:effort 15min
   complete 100
   depends !!ini.IniPro
          }
  }

  # En este punto se arrancan las tareas de recopilación
  task rec 'Recopilación' {

allocate jljerez {mandatory}
priority 1000
```

```
          # Registro de incidencias.
          task CdC 'Cadena de custodia' {
               plan:effort 2.0h
               actual:effort 55min
   complete 100
   depends !!idn
          }
  }

  # En este punto se arrancan las tareas de preservación
  task pre 'Preservación' {

allocate jljerez {mandatory}
priority 1000

          # Registro de incidencias.
          task dePre 'Dedicación a preservación' {
               plan:effort 2.0h
               actual:effort 15min
   complete 100
   depends !!rec
          }
  }

  # En este punto se arrancan las tareas de análisis
  task ana 'Análisis' {

allocate jljerez {mandatory}
priority 1000

        # Checklist de aplicaciones SW y dispositivos HW requeridos para la
        # investigación.
        task ChkHwSw 'Checklist HW/SW' {
        depends !!pre.dePre
             plan: effort 5.0h
        actual:effort 385min
        complete 100
           }

        # Checklist de artefactos
        task ChkAr 'Checklist artefctos' {
        depends !!pre.dePre
             plan: effort 2.5h
        actual:effort 180min
        complete 100
           }

#  Análisis de datos y evidencias
```

```
                task anaDE 'Análisis de datos y evidencias' {
                     plan:effort 3d
                     actual:effort 3905min
           complete 100
           depends !!pre.dePre
                }

                # Timeline (Cronología del suceso).
                task tmLi 'Timeline' {
                     plan:effort 5.0h
                     actual:effort 355min
           complete 100
           depends !anaDE
                }
       }

          # Desarrollo de la consolidación de la investigación
          task cons 'Consolidación' {

        allocate jljerez {mandatory}
                priority 1000
        depends !ana

                # Informe técnico
                task infTec 'Informe técnico' {
                     plan:effort 2d
           actual:effort 2050min
           complete 100
                }

                # Documentación: Aceptación de fin de proyecto.
                task pocFin 'Aceptación de fin' {
              plan:effort 1.0h
                       actual:effort 30min
              depends !infTec
              complete 100
            }
          }
}
}

supplement resource jljerez {
     # actual:booking $NOMB_TAREA$ $YYYY-MM-DD$-$HORA_INICIO HH:MM$-+0100 + $TRABAJO_EFECTIV
     # EJEMPLO
     # actual:booking soc.infrae.t118 2013-02-11-14:45-+0100 + 3.75h,
     #              2013-02-12-09:00-+0100 + 4.5h,
     #              2013-02-12-14:30-+0100 + 4.0h { overtime 2 }


actual:booking pfc_PoC.poc.ini.RegAcc 2015-05-26-23:55 + 5.0min
```

```
actual:booking pfc_PoC.poc.ini.planP 2015-05-27-00:05 + 5.0min
actual:booking pfc_PoC.poc.ini.planP 2015-05-27-00:15 + 20.0min
actual:booking pfc_PoC.poc.ini.planP 2015-05-27-07:35 + 400.0min
actual:booking pfc_PoC.poc.ini.planP 2015-05-27-15:30 + 390.0min

actual:booking pfc_PoC.poc.ini.EstrDir 2015-05-28-00:05 + 10.0min

actual:booking pfc_PoC.poc.ini.AcuConf 2015-05-28-19:35 + 20.0min

actual:booking pfc_PoC.poc.ini.Ant 2015-05-28-21:15 + 25.0min
actual:booking pfc_PoC.poc.ini.Ant 2015-05-29-23:30 + 5.0min

actual:booking pfc_PoC.poc.ini.InfGen 2015-05-29-23:35 + 25.0min

actual:booking pfc_PoC.poc.ini.Aut 2015-05-30-07:50 + 20.0min

actual:booking pfc_PoC.poc.ini.RegExc 2015-06-04-01:15 + 70.0min

actual:booking pfc_PoC.poc.ini.IniPro 2015-06-05-20:55 + 50.0min
actual:booking pfc_PoC.poc.ini.IniPro 2015-06-06-10:05 + 35.0min

actual:booking pfc_PoC.poc.idn.regInc 2015-06-12-10:20 + 10.0min

actual:booking pfc_PoC.poc.idn.idPaCl 2015-06-6-12:05 + 15.0min

actual:booking pfc_PoC.poc.idn.idAc 2015-06-12-17:05 + 5.0min
actual:booking pfc_PoC.poc.idn.idAc 2015-06-12-17:10 + 105.0min

actual:booking pfc_PoC.poc.idn.crEs 2015-06-13-11:55 + 40.0min
actual:booking pfc_PoC.poc.idn.crEs 2015-06-13-11:15 + 15.0min
actual:booking pfc_PoC.poc.idn.crEs 2015-06-13-23:55 + 30.0min

actual:booking pfc_PoC.poc.idn.idAI 2015-06-13-17:30 + 15.0min

actual:booking pfc_PoC.poc.rec.CdC 2015-06-14-10:55 + 55.0min

actual:booking pfc_PoC.poc.pre.dePre 2015-06-14-13:55 + 15.0min

actual:booking pfc_PoC.poc.ana.ChkHwSw 2015-06-15-15:20 + 300.0min
actual:booking pfc_PoC.poc.ana.ChkHwSw 2015-06-15-13:05 + 85.0min

actual:booking pfc_PoC.poc.ana.ChkAr 2015-06-15-20:20 + 180.0min

actual:booking pfc_PoC.poc.ana.anaDE 2015-06-16-07:35 + 380.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-16-14:30 + 390.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-16-22:00 + 240.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-17-09:35 + 205.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-17-14:00 + 670.0min
```

```
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-18-08:00 + 345.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-18-14:25 + 725.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-19-07:55 + 435.0min
actual:booking pfc_PoC.poc.ana.anaDE 2015-06-19-17:05 + 515.0min

actual:booking pfc_PoC.poc.ana.tmLi 2015-06-20-07:40 + 355.0min

actual:booking pfc_PoC.poc.cons.infTec 2015-06-20-14:10 + 690.0min
actual:booking pfc_PoC.poc.cons.infTec 2015-06-21-07:45 + 350.0min
actual:booking pfc_PoC.poc.cons.infTec 2015-06-21-15:30 + 620.0min
actual:booking pfc_PoC.poc.cons.infTec 2015-06-22-07:50 + 390.0min

actual:booking pfc_PoC.poc.cons.pocFin 2015-06-22-15:20 + 30.0min

}
```

Estructura de directorios de trabajo

Si bien cada cual es libre de crear la estructura de proyecto que crea más adecuada, en este caso, siguiendo la metodología se crea la estructura de directorios:

```
- ~pfc - poc-pfc-001~
 + ~0_inf_base~
 + ~1_planificacion~
 + ~2_inicio~
 + ~3_evidencias~
 + ~4_informes~
 + ~5_fin~
```

la creación de la estructura de directorios se ha realizado utilizando la shell interactiva de emacs como puede verse en la siguiente imagen.

Acuerdo de confidencialidad

Toda investigación digital tiene connotaciones de confidencialidad que deben de tenerse en cuenta desde el inicio de la relación entre las partes. Por ello, la firma de un documento que establezca las condiciones de la colaboración entre las partes facilita el futuro entendimiento en caso de posibles incidentes futuros relativos a la confidencialidad de los datos obtenidos durante la investigación.
El acuerdo de confidencialidad creado y que sería entregado al cliente previo al inicio de la investigación está accesible a través del siguiente enlace:

```
#+TITLE: ACUERDO DE CONFIDENCIALIDAD Y SECRETO
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:2 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
```

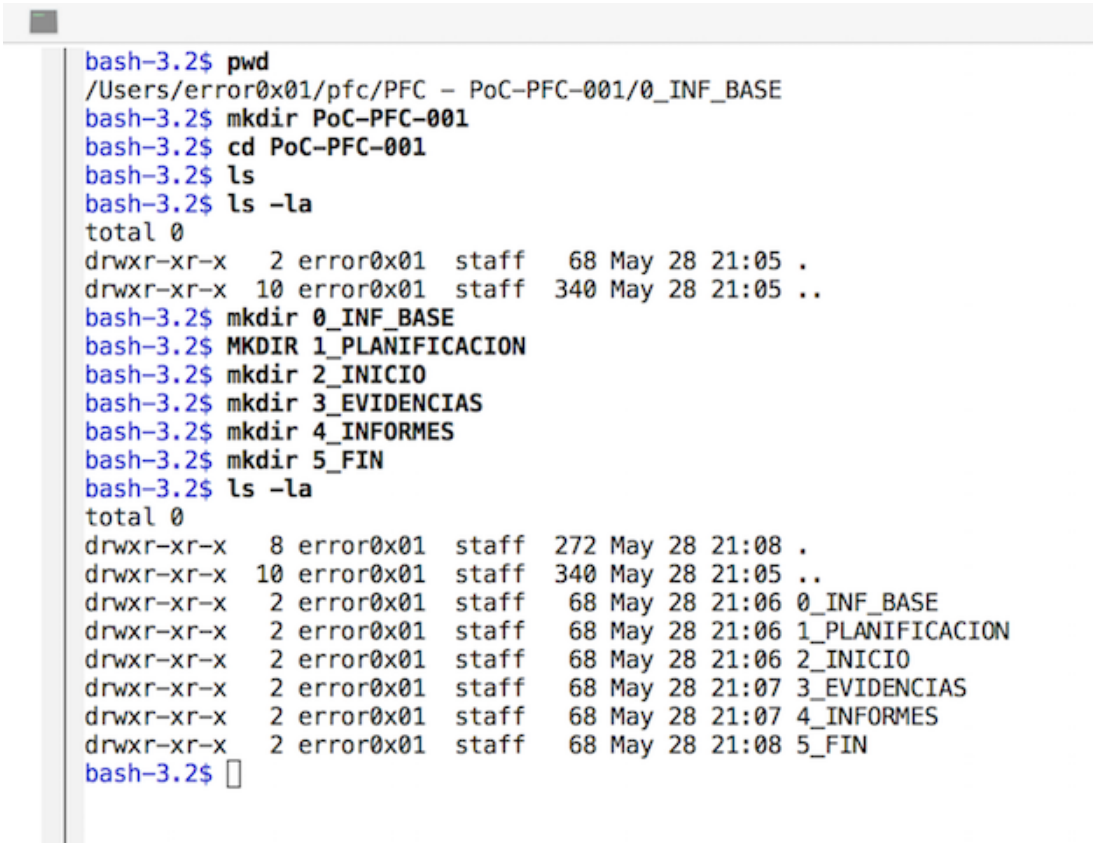


Figura 1: Emacs shell

```
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='./DOC_ANEXA/notebook.css' />

En {{{provinciaCli}}}, a {{{date(%d-%m-%Y)}}}.

* REUNIDOS

D./Dª {{{nomCli}}}, mayor de edad, con domicilio en la C/{{{calleCli}}}
Nº {{{numCli}}}, Localidad {{{localidadCli}}} Provincia {{{provinciaCli}}} C.P. {{{codCli}}} con
D.N.I. {{{dniCli}}}, y en representación de la compañía {{{empCli}}}, con
CIF {{{cifCli}}} y domicilio social en {{{provinciaCli}}} y,

D./Dª {{{nomProf}}}, mayor de edad, con domicilio en la C/{{{calleProf}}}
Nº {{{numProf}}}, Localidad {{{localidadProf}}} Provincia {{{provinciaProf}}} C.P. {{{codProf}}}
D.N.I. {{{dniProf}}}, y en representación de la compañía {{{empProf}}}, con
CIF {{{cifProf}}} y domicilio social en {{{provinciaProf}}}.

* EXPONEN
```

1. Que ambas partes se reconocen capacidad jurídica suficiente para suscribir el presente documento.

2. Que ambas partes desean iniciar una relación negocial y de colaboración mutua a nivel empresarial.

3. Que durante la mencionada relación las partes intercambiarán o crearán información que están interesadas en regular su confidencialidad y secreto mediante las siguientes:

* CONDICIONES
** I. OBJETO

Con el presente contrato las partes fijan formalmente y por escrito los términos y condiciones bajo las que las partes mantendrán la confidencialidad de la información suministrada y creada entre ellas.

Que a los efectos de este acuerdo, tendrá la consideración de información confidencial, toda la información susceptible de ser revelada por escrito, de palabra o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro, intercambiada como consecuencia de este acuerdo.

Este acuerdo no constituye ningún acuerdo de licencia, contrato de desarrollo o similar, obligándose las partes a adoptar las medidas oportunas para asegurar el tratamiento confidencial de dicha información, medidas que no serán menores que las aplicadas por ellas a la propia información confidencial de su compañía.

** II. DURACIÓN

Este acuerdo tendrá una duración indefinida desde el momento de su firma.

En caso de que no se renueve el contrato, ambas partes deberán devolver a la otra toda la información remitida entre sí, comprometiéndose a la destrucción de cualquier copia de la misma, independientemente del soporte o formato en el que se encuentre almacenada.

No obstante, lo dispuesto en el párrafo anterior, cada parte se compromete a mantener el compromiso de confidencialidad respecto a la información y material intercambiado entre las partes, de forma indefinida tras la finalización del presente acuerdo.

** III. CONFIDENCIALIDAD

Las partes se obligan a entregarse todo el material que sea necesario, y en el caso de ser este confidencial se comprometen a:

a. Utilizar dicha información de forma reservada.

b. No divulgar ni comunicar la información técnica facilitada por la otra parte.

c. Impedir la copia o revelación de esa información a terceros, salvo que gocen de aprobación escrita de la otra parte, y únicamente en términos de tal aprobación.

d. Restringir el acceso a la información a sus empleados y subcontratados, en la medida en que razonablemente puedan necesitarla para el cumplimiento de sus tareas acordadas.

e. No utilizar la información o fragmentos de ésta para fines distintos de la ejecución de este contrato.

Las partes serán responsables entre sí, ante el incumplimiento de esta obligación, ya sea por sus empleados o por subcontratados.

Las partes mantendrán ésta confidencialidad y evitarán revelar la información a toda persona que no sea empleado o subcontratado, salvo que:

a. La parte receptora tenga evidencia de que conoce previamente la información recibida.

b. La información recibida sea de dominio público.

c. La información recibida proceda de un tercero que no exige secreto.

** IV. DERECHOS PREVIOS SOBRE LA INFORMACIÓN

Toda información puesta en común entre las partes es de propiedad exclusiva de la parte de donde proceda, y no se precisa la concesión de licencia para dicho intercambio. Ninguna de las partes utilizará información previa de la otra parte para su propio uso, salvo que se autorice lo contrario.

La información que se proporciona no da derecho o licencia a la empresa que la recibe sobre las marcas, derechos de autor o patentes que pertenezcan a quien la proporciona. La divulgación de información no implica transferencia o cesión de derechos, a menos que se redacte expresamente alguna disposición al respecto.

** V. CLÁUSULA PENAL

Las partes se comprometen a cumplir con todos los términos fijados en el presente contrato, y muy especialmente aquellos relativos a las

cláusulas sobre propiedad intelectual e industrial, confidencialidad y obligación de secreto.

Independientemente de las responsabilidades que pudieran derivarse del incumplimiento del presente acuerdo, así como de las eventuales indemnizaciones por daños y perjuicios de cualquier naturaleza que pudieran establecerse, el incumplimiento de estas obligaciones determinará a elección de la parte que no incumplió el contenido de los términos fijados en el presente contrato:

a. La resolución del contrato.

b. El abono de {{{costeIncumplimiento}}} € en concepto de penalización.

** VI. DERECHOS DE PROPIEDAD

Toda información intercambiada es de propiedad exclusiva de la parte de la cual proceda. Ninguna de las partes utilizará información de la otra para su beneficio independiente.

** VII. PROTECCIÓN DE DATOS

Para la correcta aplicación del presente acuerdo, ambas partes podrían tener acceso a datos de carácter personal protegidos por la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, por lo que se comprometen a efectuar un uso y tratamiento de los datos afectados que será acorde a las actuaciones que resulten necesarias para la correcta prestación de servicios regulada en este acuerdo, según las instrucciones facilitadas en cada momento.

Asimismo, las partes asumen la obligación de guardar secreto profesional sobre cuanta información pudieran recibir, gestionar y articular con relación a los datos personales y a no comunicarlos a terceros, salvo las excepciones mencionadas, así como a destruirlos, cancelarlos o devolverlos en el momento de la finalización de la relación contractual entre ambas partes, así como a aplicar las medidas de seguridad necesarias.

Los derechos de acceso, rectificación, cancelación y oposición podrán ejercitarse mediante escrito dirigido a las direcciones de los firmantes del presente documento que constan en el encabezamiento.

** VIII. CONFIDENCIALIDAD DEL ACUERDO

Las partes acuerdan que este acuerdo reviste el carácter de confidencial y por tanto se prohíbe su divulgación a terceros.

** IX. MODIFICACIÓN O CANCELACIÓN

```
Este acuerdo sólo podrá ser modificado con el consentimiento expreso de
ambas partes, en documento escrito y mencionando la voluntad de las
partes de modificar el presente acuerdo.

**   X. JURISDICCIÓN.

Las partes se comprometen a resolver de manera amistosa cualquier
desacuerdo que pueda surgir en el desarrollo del presente contrato.

En caso de conflicto ambas partes acuerdan el sometimiento a los
Tribunales de {{{Lugar}}}, con renuncia de su propio fuero.

Y en prueba de conformidad de cuanto antecede, firman el presente
acuerdo por duplicado y a un solo efecto en el lugar y fecha citados.

Firmado en {{{provinciaCli}}} a {{{date(%d-%m-%Y)}}}.
```

El fichero puede ser accedido mediante el enlace

Antecedentes de la investigación

La información relativa a los antecedentes se obtiene a partir de los datos que aparecen en el enlace `http://www.seguridad.unam.mx/eventos/reto/` y se ha concretado con el siguiente formato:

```
#+TITLE: ANTECEDENTES
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:t -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil title:nil
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)

*Código de documento:* PoC-ATC-001

*Lugar de reunion:* {{{calleProf}}}

*Objetivo:* Obtener la información referente a los antecedentes de la
investigación.

*Responsable de la reunion:*  {{{nomCli}}}

*Fecha y Hora de inicio:* [2015-05-29 Fri 15:01]

*Fecha y Hora de fin:* [2015-05-29 Fri 18:22]

*Clasificación:* CONFIDENCIAL
```

Asuntos a tratar:

 - Sucesos identificados.
 - Personal implicado.
 - Sistemas implicados.

ASISTENTES

Nombre	Cargo
{{{nomCli}}}	{{{cargoCli}}}
{{{nomProf}}}	{{{tipoProf}}}

Observaciones:

En el caso que nos ocupa, no hay información adicional ni oportunidad de obtenerla.

La información relativa a los antecedentes se obtiene a
partir del enlace http://www.seguridad.unam.mx/eventos/reto/.

Proxima reunion: No establecida

ANTECEDENTES

Num	Descripcion
1	El administrador de sistemas de una pequeña empresa ha notado que existe una cuenta que él no creó en su sistema de ERP (Enterprise Resource Planning), por lo que el administrador de sistemas sospecha de algún ingreso no autorizado, del que desconoce el alcance.
2	El sistema en que se ejecuta la aplicación es un servidor Windows 2003, cuya principal función era proporcionar acceso al sistema ERP a través de la Web.
3	Hace poco tiempo que habían migrado al uso de este servidor.
4	Según el administrador, trataba de mantener el sistema actualizado por lo que no sabe cómo pudieron

	ingresar a su sistema.
5	El administrador mencionó que más de una persona tiene acceso a cuentas privilegiadas en el sistema y que a veces utilizan estas cuentas para labores administrativas y personales.
6	El administrador mencionó que los usuarios del servidor utilizan aplicaciones que no requieren ningún tipo de privilegio para ejecutarse.
7	Datos de la imagen del equipo comprometido: - Sistema Operativo de equipo comprometido: Windows 2003 - Tamaño de la imagen: <= 6 GB. - La firmas md5 de la imagen completa, comprimida y descomprimida, respectivamente, son: + 062cf5d1ccd000e20cf4c006f2f6cce4 - windows2003.img + 33a42d316c060c185f41bfcacf439747 - windows2003.img.gz

COMENTARIOS DEL INVESTIGADOR

Num	Descripcion
1	No se especifica ningún dato adicional acerca del ERP.
2	No se especifica ningún dato adicional acerca del servdor, como el nivel de parcheo o funcionalidades/aplicaciones adicionales del servidor que podrían ser relevantes para la investigación.
3	No se facilitan fechas, concretas ni aproximadas, relativas a la instalación o posible intrusión.
4	No se facilita información concreta acerca del nivel de parches instalados en el sistema o aplicativos instalados.
5	No se facilita un listado de usuarios con acceso al sistema (ni por lo tanto sus contraseñas).

COMPROMISOS/ACUERDOS

Num	Descripcion	Responsable	Fecha
1	firmar el documento de aceptación y	{{{nomProf}}}	

	autorización de trabajos		
2			
3			

El documento de antecedentes es accesible en el siguiente enlace:

Datos generales de la investigación

El fichero de datos de la investigación se va cumplimentando a medida que avanza la misma y en función de los ficheros que se generan utilizando las distintas plantillas desarrolladas.
Dado que en el momento inicial en el que se requiere esta documentación solo se dispondrían de los datos de contacto del cliente y una idea general del alcance del proyecto, este documento se desarrollará en distintos momentos.

```
#+MACRO: nomProf José Luis Jerez
#+MACRO: cargoProf Investigador forense
#+MACRO: dniProf 12345678-x
#+MACRO: cifProf A-87654321
#+MACRO: calleProf C/Eureka
#+MACRO: numProf 10
#+MACRO: localidadProf Las Rozas
#+MACRO: provinciaProf Madrid
#+MACRO: codProf 28231
#+MACRO: empCli Red Iris
#+MACRO: nomCli Francisco Monserrat
#+MACRO: cargoCli Responsable del reto forense
#+MACRO: dniCli 66666666-D
#+MACRO: cifCli B-99999999
#+MACRO: calleCli Plaza de Manuel Gómez Moreno, s/n - 2a planta
#+MACRO: numCli 1
#+MACRO: localidadCli Madrid
#+MACRO: provinciaCli Madrid
#+MACRO: codCli 94043
#+MACRO: telCli (+34) 91 212 76 25
#+MACRO: emailCli francsco.monserrat@rediris.es
#+MACRO: horaContCli 9:00 - 18:00
#+MACRO: tipoServ Investigación forense
#+MACRO: codProy IF-RIRIS-POC-001
#+MACRO: costeIncumplimiento 6.000.000
#+MACRO: fechaIni Mon Mar 18 08:00:37 CET 2013
#+MACRO: fechaFin Thu Abr 18 18:00:07 CET 2013
#+MACRO: Activo_1 Fichero 'windows2003.img.gz'
#+MACRO: numJornEsf 22
```

El fichero puede ser accedido mediante el enlace `./PoC-PFC-001/0_INF_BASE/PoC_Datos_generales.org`

Autorización y aceptación de trabajos

La firma del documento de autorización de trabajos es crítica para el correcto arranque de la investigación y ésta no debe de iniciarse sin disponer del documento correctamente cumplimentado y formado.
El documento debe de responder a las cuestiones básicas que considere el investigador tras conocer los antecedentes, tales como ¿cuál es el escenario ante el que hay que enfrentarse?, ¿qué quiere analizarse: un fichero, un directorio, un disco o todo un sistema?, ¿dónde y cómo se almacenarán las evidencias?, ¿cuántas copias deben realizarse? y cualquier dato relevante que daba establecerse previo al inicio de las actividades de investigación propiamente dichas.

```
#+TITLE: AUTORIZACIÓN DE TRABAJOS
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:t -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)

El presente acuerdo presume la previa aceptación de la oferta asociada
al proyecto con código {{{codProy}}} según los términos expresados en la
misma.

Se autoriza a {{{nomProf}}} a realizar los trabajos de {{{tipoServ}}}
sobre los activos identificados por {{{empCli}}}, permitiendo efectuar
las pruebas correspondientes.

Activos a analizar:

- {{{Activo_1}}}

Siguiendo la metodología DIEM de investigación digital se realizarán las
copias de seguridad necesarias para la preservación de las evidencias y
las mismas serán almacenadas siguiendo un procedimiento que permita
asegurar la integridad y trazabilidad de las mismas.

Toda la investigación se realizará respetando la legislación vigente así
como las políticas de {{{empCli}}}, y manteniendo las medidas de
confidencialidad descritas en la metodología.

Para que conste, se emite la presente autorización por el Responsable de
Seguridad la Empresa {{{empCli}}}.

D/Dª. {{{nomCli}}}
```

```
En {{{provinciaCli}}} a {{{date(%d-%m-%Y)}}}.
```

Para el caso que nos ocupa se ha cumplimentado la plantilla general de forma que el texto queda siguiente modo:

Registro de exclusiones

Tras revisar el contexto legal y humano de la investigación y el escenario a analizar se observan las siguientes exclusiones que limitan la misma:

```
#+tblname: POC-051114-001
|------------------+-----------------------------------------------------|
| Código           | POC-051114-001                                      |
|------------------+-----------------------------------------------------|
| Exclusion/limite | Se excluye cualquier tipo de fuente de evidencias   |
|                  | adicional a la imagen facilitada.                   |
|------------------+-----------------------------------------------------|
| Motivo           | Reglas del reto forense.                            |
|------------------+-----------------------------------------------------|
| Responsable      | Organización del reto.                              |
|------------------+-----------------------------------------------------|

#+tblname: POC-051114-002
|------------------+-----------------------------------------------------|
| Código           | POC-051114-002                                      |
|------------------+-----------------------------------------------------|
| Exclusion/limite | Se excluyen entrevistas o información adicional     |
|                  | por parte del cliente.                              |
|------------------+-----------------------------------------------------|
| Motivo           | Reglas del reto forense.                            |
|------------------+-----------------------------------------------------|
| Responsable      | Investigador.                                       |
|------------------+-----------------------------------------------------|

#+tblname: POC-081114-001
|------------------+-----------------------------------------------------|
| Código           | POC-081114-001                                      |
|------------------+-----------------------------------------------------|
| Exclusion/limite | Se excluye el acceso a datos personales localizados |
|                  | en la imagen facilitada.                            |
|------------------+-----------------------------------------------------|
| Motivo           | Contexto legal.                                     |
|------------------+-----------------------------------------------------|
| Responsable      | Investigador.                                       |
|------------------+-----------------------------------------------------|
```

El documento origen del registro de exclusiones está accesible en `./PoC-PFC-001/0_INF_BASE/PoC-RE-001.org`

Documento de inicio de proyecto

Siguiendo la recomendación de la metodología, para el desarrollo del documento de inicio de proyecto se realiza una copia de la plantilla original previamente al inicio de la modificación de la misma.
Se valida que el documento de datos generales dispone de todos los datos necesarios para la importación de los mismos y se desarrollan los apartados concretos cuyos datos, debido a la extensión de los mismos, no van a ser importados.
Una vez se dispone del documento modificado tal y como aparece a continuación se utiliza la función `gpgFilesToPDF` para su exportación segura a PDF.

```
#+TITLE: DOCUMENTO DE INICIO DE PROYECTO
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:2 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='./DOC_ANEXA/notebook.css' />

* Categorización del proyecto

/Código de Proyecto:/ {{{codProy}}}

/Profesional contratado:/ {{{nomProf}}}

/Referencia:/

La investigación actual llegó al profesional contratado por elección
propia a la hora de seleccionar una prueba de concepto para el
desarrollo del proyecto fin de carrera.

/Antecedentes:/

En este caso se ha desarrollado un [[./PoC-ATC-001.org.pdf][fichero de antecedentes]] donde se
describen los detalles del mismo.

No se conocen detalles adicionales en el momento del desarrollo del
documento de inicio de proyecto.

/Objetivo del proyecto:/

Analizar la imagen de la máquina virtual facilitada y facilitar
objetivamente, en función de las evidencias obtenidas aplicando un
```

proceso metodológico adecuado a la legalidad de un procedimiento penal, información relativa a la posibilidad de que se haya producido una intrusión.

/Alcance del Proyecto:/

- {{{Activo_1}}}

/Requisitos previos:/

- Firma de la documentación relativa a autorizaciones y permisos para el desarrollo de la investigación en función de la metodología aplicada.
- Disponer de toda la información conocida por parte del cliente acerca de la intrusión.
- Disponer de la imagen de la máquina virtual.
- El cliente debe de facilitar sus políticas.
- El cliente debe de informar de cualquier limitación al alcance de la investigación que quede fuera del contexto de las limitaciones legales, si existiesen.

* Ficha cliente

/Empresa:/ {{{empCli}}}

/Persona responsable en el Cliente:/ {{{nomCli}}}

/Teléfono de contacto:/ {{{telCli}}}

/Correo electrónico:/ {{{emailCli}}}

/Dirección del proyecto:/ {{{calleCli}}}, {{{localidadCli}}}, {{{provinciaCli}}}

/Horario de contacto:/ {{{horaContCli}}}

* Planificación

/Fecha de Inicio:/ {{{fechaIni}}}

/Fecha de fin:/ {{{fechaFin}}}

/Esfuerzo previsto:/ {{{numJornEsf}}} jornadas

/Posibles interrupciones previstas:/

A priori no se esperan interrupciones durante el proceso de la investigación.

/Aspectos críticos del proyecto:/

```
No se identifican aspectos críticos que deban de ser conocidos y
aceptados por el cliente. Si bien se le ha informado de que el actual
proyecto va a ser desarrollado exclusivamente utilizando Emacs y las
herramientas que puedan ser ejecutadas desde este entorno.

* Aceptación del inicio del proyecto

Responsable de proyecto: {{{nomCli}}}

#+BEGIN_EXAMPLE

Firma:
```

de la empresa .
Fecha: 7 de julio de 2015
#+END_EXAMPLE

Registro de incidencias

El documento de registro de incidencias se crea en el momento es el que es requerido, por lo que no es un documento asociado al proceso de identificación. Sin embargo, a pesar de que en el momento de crearlo en la investigación que nos ocupa no se ha dado ninguna incidencia, creo que es importante disponer del mismo desde el inicio aunque en este momento carezca de contenidos.
Por otro lado, si finaliza el proyecto sin incidencias, es importante disponer de dicho documento para que se disponga de una evidencia que refuerce el argumento de que la investigación se ha iniciado y finalizado sin incidencias.

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Código del Proyecto {{{codProy}}}

|-----+----------------+--------------+-------------+--------+------------+--------+-------------
| No. | Descripción de | Fecha        | Responsable | Estado | Fecha      | Fecha  | Observacione
|     | la incidencia  | notificación |             |        | resolución | cierre |
|-----+----------------+--------------+-------------+--------+------------+--------+-------------
|   1 |                |              |             |        |            |        |
|-----+----------------+--------------+-------------+--------+------------+--------+-------------
|   2 |                |              |             |        |            |        |
```

```
|-----+---------------+-------------+------------+--------+-----------+--------+--------
```

```
NOTA: Para las fechas ver [[file:5_emacs.org::*Gesti%C3%B3n%20del%20tiempo][Gestión del tiem
```

Identificación de palabras clave

En este punto ya se puede decir objetivamente que se ha iniciado la investigación como tal.
Los elementos y palabras clave son los que se extrapolan del texto de antecedentes, si bien este documento se ampliará a medida que se avance en la investigación.

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />
```

```
Código del Proyecto {{{codProy}}}
```

```
|-----+-------------------------+-----------------------------------------------|
| No. | Palabras clave          | Observaciones                                 |
|-----+-------------------------+-----------------------------------------------|
|   1 | Sistema de ERP          | Enterprise Resource Planning                  |
|-----+-------------------------+-----------------------------------------------|
|   2 | Cuenta comprometida ERP | No se facilita la cuenta                      |
|-----+-------------------------+-----------------------------------------------|
|   3 | Windows 2003            | Sistema operativo del servidor comprometido   |
|-----+-------------------------+-----------------------------------------------|
|   4 | Actualizaciones del SO  | El sistema se trataba de mantener actualizado |
|-----+-------------------------+-----------------------------------------------|
|   5 | Cuentas privilegiadas   | No se facilitan las cuentas                   |
|     |                         | Con permisos de administración                |
|     |                         | Se utilizan para labores personales           |
|-----+-------------------------+-----------------------------------------------|
|   6 | Aplicaciones de usuario | No se especifican las aplicaciones            |
|     | instaladas              |                                               |
|-----+-------------------------+-----------------------------------------------|
```

Identificación de actores

Los actores iniciales son los que se extrapolan del texto de antecedentes, si bien este documento se ampliará a medida que se avance en la investigación y se identifiquen nuevos actores.

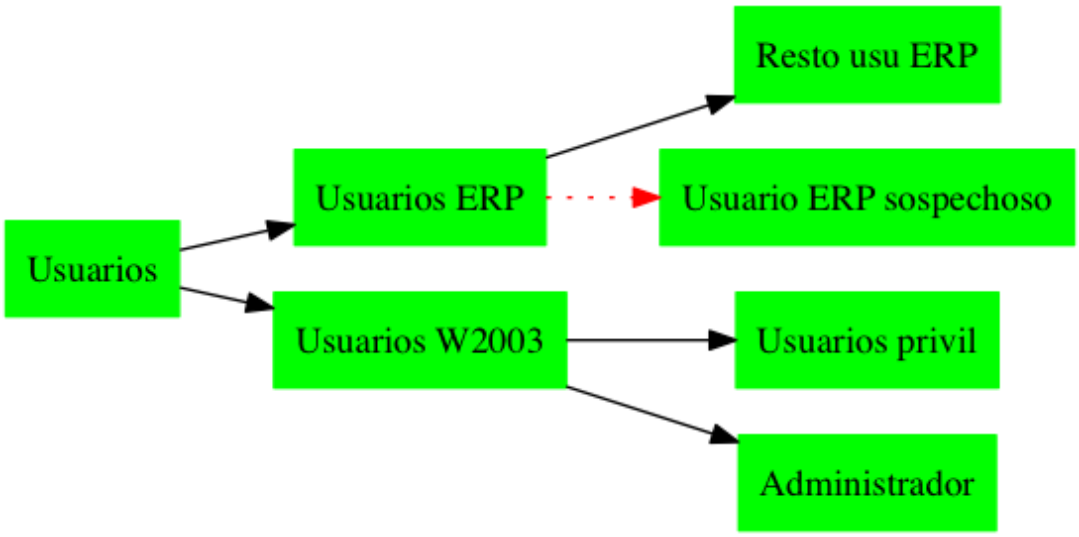
```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Código del Proyecto {{{codProy}}}

|-----+--------------------------+-----------------------------------------------------|
| No. | Actores                  | Observaciones                                       |
|-----+--------------------------+-----------------------------------------------------|
|   1 | Administrador            |                                                     |
|-----+--------------------------+-----------------------------------------------------|
|   2 | Empleados con acceso al  | Disponen de cuentas con permiso de administración |
|     | servidor                 | en el sistema                                       |
|-----+--------------------------+-----------------------------------------------------|
|   3 | *Usuario ERP sospechoso* | Cuenta no controlada por el administrador. Se     |
|     |                          | desconoce su origen.                                |
|-----+--------------------------+-----------------------------------------------------|
```

Identificación del cuadro relacional

En este caso he utilizado Graphviz para diseñar el cuadro relacional ya que la integración con Emacs es inmediata y sencilla. Sin embargo otra tecnología más actual que también podría utilizarse es Neo4j.
La idea es utilizar una tecnología que se pueda desarrollar en modo texto y que posteriormente, utilizando Emacs, se transforme en un gráfico que relaciones los distintos actores.

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Código del Proyecto {{{codProy}}}
```

```
#+BEGIN_SRC dot :file cuadro_relacional.png :cmdline -Kdot -Tpng
  digraph {
  // graph from left to right
  rankdir=LR;
  splines=true;
  node [shape=box,style=filled,color=green]

  us [label='Usuarios']
  use [label='Usuarios ERP']
  usw [label='Usuarios W2003']
  usp [label='Usuarios privil']
  ad [label='Administrador']
  re [label='Resto usu ERP']


  us -> use
  us -> usw
  use -> 'Usuario ERP sospechoso' [style=dotted][color=red]
  use -> re
  usw -> ad
  usw -> usp
  }

#+END_SRC

#+RESULTS:
[[file:cuadro_relacional.png]]
```



Croquis del escenario integrando todos los elementos

En este caso no tiene sentido el croquis del escenario dado que no hay ningún espacio físico que fotografiar y en el que podamos identificar los indicios mediante tarjetas numeradas, pero con el fin de que el proceso sea lo más realista posible se realizará una simulación de los hechos.

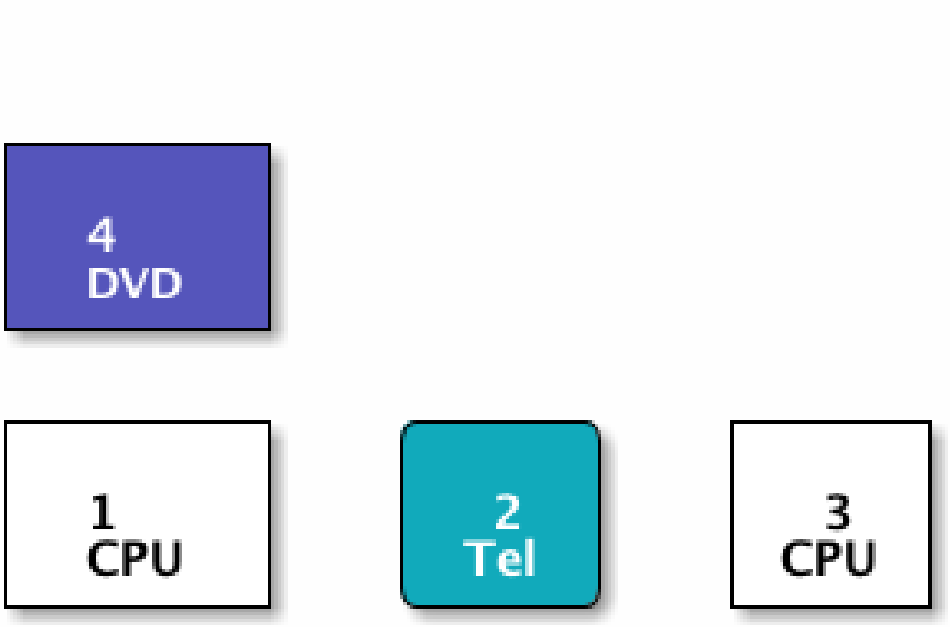
Sin embargo, a modo de ejemplo, a continuación se puede ver una fotografía de un escenario simulado donde se encuentra el servidor comprometido así como otros elementos informáticos que, al encontrarse en el escenario a investigar, también deben de ser documentados. Cada uno de ellos debe de aparecer identificado con una etiqueta indicativa de marcado tal como se explica en la metodología, si bien en este caso las etiquetas que deberían de estar físicamente en el escenario se han añadido digitalmente.

Figura 2: Escenario fotografiado

En este caso también tendríamos que hacer una fotografía de la pantalla tal como la encontramos e incluso identificarla adecuadamente.

El escenario presentado se representa igualmente en un croquis desarrollado con Emacs siguiendo la metodología, utilizando `ditaa`, como el que se puede ver a continuación.

```
#+BEGIN_SRC ditaa :file IMG/croquis.png

   +--------+
   |cBLU    |
   |  4     |
   |  DVD   |
   +--------+

   +--------+    /-----\    +------+
   |        |    |c1AB |    |      |
   |  1     |    |  2  |    |  3   |
   |  CPU   |    | Tel |    | CPU  |
   +--------+    \-----/    +--+---+


#+END_SRC

#+RESULTS:
[[file:IMG/croquis.png]]
```



Identificación de activos involucrados

Los activos involucrados son los que se extrapolan del texto de antecedentes, si bien este documento, en otro contexto, se podría ampliar a medida que se avance en la investigación.
Los códigos identificativos deben de corresponderse con los identificadores de las fotografías y de los croquis si existe relación entre las mismas.
No es necesario dar mayor detalle de los activos ya que éstos se documentan en el documento de cadena de custodia a partir del momento en que son recolectados o adquiridos.

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Código del Proyecto {{{codProy}}}

|-----+---------------+-------------------------------------|
| No. | Activos       | Observaciones                       |
|-----+---------------+-------------------------------------|
```

```
|   1 | CPU            | Equipo de trabajo del administrador |
|-----+----------------+-------------------------------------|
|   2 | Teléfono móbil | Teléfono móbil del administrador    |
|-----+----------------+-------------------------------------|
|   3 | CPU            | Servidor corporativo                |
|-----+----------------+-------------------------------------|
|   4 | DVD            |                                     |
|-----+----------------+-------------------------------------|
```

Para el caso de la prueba de concepto, dado que nuestro único activo identificado es la imagen facilitada por el cliente, el documento de identificación de activos involucrados sería:

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Código del Proyecto {{{codProy}}}

|-----+----------------------------------+----------------------------|
| No. | Activos                          | Observaciones              |
|-----+----------------------------------+----------------------------|
|   1 | Imagen del servidor Windows 2003 | Fichero windows2003.img.gz |
|-----+----------------------------------+----------------------------|
```

Cadena de custodia

De los activos involucrados que aparecen en el apartado anterior se debería de crear, por cada uno de ellos, un documento de cadena de custodia.
En la investigación en curso el único activo recopilado es la imagen de disco (windows2003.img.gz) facilitada por el cliente, por lo que sólo se va a desarrollar un documento de cadena de custodia.
Si bien este documento se inicia dentro del proceso de recopilación, es un documento que permanece en constante evolución a lo largo del proyecto y mientras s siga tratando la evidencia a la que referencia.
El correcto tratamiento de dicho documento es crítico a la hora de asegurar la validez de la evidencia frente a cualquier jurado.

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
```

```
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Código del Proyecto {{{codProy}}}

|-------------------+-----------------------------------------+-------------------------|
|                   | Datos                                   | Observaciones           |
|-------------------+-----------------------------------------+-------------------------|
| Código            | 1                                       | Ver PoC-IAI-001.pdf     |
|-------------------+-----------------------------------------+-------------------------|
| Activo            | {{{Activo_1}}}                          | Fichero comprimido      |
|-------------------+-----------------------------------------+-------------------------|
| Hash              | 2f53bf2187ce9efcb1ec0e7f930141b36f2f7dc9 | bash-3.2$ shasum -v     |
|                   |                                         | 5.84                    |
|-------------------+-----------------------------------------+-------------------------|
| Fecha recopilación | [2015-06-14 Sun 10:59]                  |                         |
|-------------------+-----------------------------------------+-------------------------|
| Forma de recopil. | recolección                             | No se dispone de        |
|                   |                                         | notario ni fedatario    |
|                   |                                         | público.                |
|-------------------+-----------------------------------------+-------------------------|
| Tamaño (bytes)    | 3500527266                              | El fichero descomprimido |
|                   |                                         | ocupa 5239471104 bytes  |
|-------------------+-----------------------------------------+-------------------------|
| Número de copias  | 3 copias disponibles                    | 1 en la web             |
|                   |                                         | 1 en servidor NAS       |
|                   |                                         | 1 de trabajo            |
|-------------------+-----------------------------------------+-------------------------|
| Responsable       | {{{nomProf}}}                           | {{{cargoProf}}}         |
|-------------------+-----------------------------------------+-------------------------|
```

Checklist de herramientas HW/SW

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
```

```
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

* Documentación
- [X] Documentación de proyecto impresa
  - [X] [[~/pfc/PFC%20-%20PLANTILLAS/Acuerdo%20de%20confidencialidad.org][Acuerdo de confide
  - [X] Antecedentes
  - [X] [[~/pfc/PFC%20-%20PLANTILLAS/Autorizacio%CC%81n%20y%20aceptacio%CC%81n%20de%20trabaj
  - [X] Cadena de custodia
  - [X] Plan de proyecto
- [X] Listado de contraseñas por defecto para dispositivos (BIOS, routers, etc)
  - [X] [[~/pfc/PFC%20-%20DOC%20ANEXA/default%20passwords.pdf][default passwords.pdf]]
  - [X] [[~/pdf/PFC%20-%20DOC%20ANEXA/Network__4-Admin_List_of_default_Router_Passwords_and_
  - [X] https://cirt.net/passwords
  - [X] http://www.routerpasswords.com
* Inventario de hardware
- [X] Equipo portátil con puerto serie
- [X] Monitor
- [X] Teclado
- [X] Ratón
- [X] Dispositivo de copia de discos 2½ y 3½
- [X] Unidad de almacenamiento
  - [X] CD-ROM Lector/Gravador
  - [X] DVD Lector/Gravador
- [X] Pendrive
- [X] Grabadora de voz
- [X] Disco vírgenes
  - [X] CD
  - [X] DVD
- [X] Hub
- [X] Switch
- [X] Router wifi
- [X] Tarjeta de red
  - [X] ethernet
  - [X] wireless
- [X] UPS
- [X] Cables
  - [X] IDE 40/80 pines
  - [X] IDE de alimentación
  - [X] SATA 7 pines
  - [X] SATA alimentación
* Inventario de sistemas de arranque
- [X] CD de arranque de sistema con herramientas forenses.
- [X] DVD de arranque de sistema con herramientas forenses.
- [X] Pendrive de arranque de sistema con herramientas forenses.
* Herramientas software
- [X] [[http://forensicswiki.org/wiki/Bulk_extractor][bulk-extractor]]
  + bulk_extractor is a computer forensics tool that scans a disk image,
```

    a file, or a directory of files and extracts useful information
    without parsing the file system or file system structures. The
    results can be easily inspected, parsed, or processed with automated
    tools. bulk_extractor also creates a histograms of features that it
    finds, as features that are more common tend to be more
    important. The program can be used for law enforcement, defense,
    intelligence, and cyber-investigation applications.
- [X] [[http://afflib.sourceforge.net/][afflib-tools]]
  + Advanced Forensics Format (AFF) is an extensible open format for the
    storage of disk images and related forensic metadata.
- [X] [[http://afterglow.sourceforge.net][AfterGlow]]
  + AfterGlow is a collection of scripts which facilitate the process of
    generating link graphs. The tool is written in Perl and needs to be
    invoked via the command line.
  + As input, AfterGlow expects a CSV file.
  + A common way of generating the CSV files are parsers which take a
    raw input file, analyze it and output a comma separated list of
    records based on the data they found. The output of AfterGlow is one
    of two formats. Either it generates a dot attributed graph language
    file - the input required by the graphviz library - or it can
    generate GDF files that can, for example, be visualized with Gephi.
- [X] [[http://www.sleuthkit.org][The Sleuth Kit]]
  - Conjunto de herramientas de analisis forense de libre distribucion.
- [X] [[http://es.wikipedia.org/wiki/John_the_Ripper][John the Ripper]]
  - John the Ripper es un programa de criptografía que aplica fuerza
    bruta para descifrar contraseñas. Es capaz de romper varios
    algoritmos de cifrado o hash, como DES, SHA-1 y otros.
- [X] [[http://forensicswiki.org/wiki/Libevt][libevt]]
  - The libevt package contains a library and applications to read
    Windows Event Log (EVT) files.
  - Contains ~evtinfo~, which shows information about
    EVT files and ~evtexport~, which exports information from EVT files.
- [X] [[http://www.graphviz.org][graphviz]]
  + Graphviz is open source graph visualization software.
- [X] python
- [X] ipython
- [X] [[http://forensicswiki.org/wiki/Dc3dd][dc3dd]]
  + dc3dd is a patched version of GNU dd with added features for
    computer forensics.
- [X] [[http://forensicswiki.org/wiki/Dcfldd][dcfldd]]
  + dcfldd is an enhanced version of dd developed by the U.S. Department
    of Defense Computer Forensics Lab.
- [X] [[http://forensicswiki.org/wiki/Exif][Exif]]
  + The Exchangeable image file format (Exif) is an image file format
    which adds lots of metadata to existing image formats, mainly JPEG.
- [X] [[http://www.monkey.org/~dugsong/dsniff/][dsniff]]
  + dsniff is a collection of tools for network auditing and penetration
    testing. dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and
    webspy passively monitor a network for interesting data (passwords,

e-mail, files, etc.). arpspoof, dnsspoof, and macof facilitate the interception of network traffic normally unavailable to an attacker (e.g, due to layer-2 switching). sshmitm and webmitm implement active monkey-in-the-middle attacks against redirected SSH and HTTPS sessions by exploiting weak bindings in ad-hoc PKI.
- [X] [[http://www.thoughtcrime.org/software/sslsniff/][sslsniff]]
  + It is designed to MITM all SSL connections on a LAN, and dynamically generates certs for the domains that are being accessed on the fly.
- [X] [[http://es.wikipedia.org/wiki/Fdupes][fdupes]]
  + Fdupes es un programa para escanear directorios en busca de ficheros duplicados, con opciones para listarlos y borrarlos. Primero compara los tamaños de los ficheros y firmas MD5, y después realiza una verificación byte-a-byte.
- [X] [[http://es.wikipedia.org/wiki/Netcat][Netcat]]
  + Netcat es una herramienta de red que permite a través de intérprete de comandos y con una sintaxis sencilla abrir puertos TCP/UDP en un HOST (quedando netcat a la escucha), asociar una shell a un puerto en concreto (para conectarse por ejemplo a MS-DOS o al intérprete bash de Linux remotamente) y forzar conexiones UDP/TCP (útil por ejemplo para realizar rastreos de puertos o realizar transferencias de archivos bit a bit entre dos equipos).
- [X] [[http://es.wikipedia.org/wiki/PDFtk][PDFtk]]
  + PDFtk o the PDF toolkit es una herramienta de código abierto multiplataforma para la munipulación de documentos PDF. pdftk es básicamente un front end de la biblioteca iText(compilada a código nativo usando GCJ), capaz de dividir, combinar, cifrar, descifrar, descomprimir, recomprimir y reparar documentos PDF. Puede también ser utilizada para manipular marcas de agua, metadatos, o para llenar formularios PDF con datos FDF (Forms Data Format) o datos XFDF (XML Form Data).
- [X] [[http://www.cabextract.org.uk][cabextract]]
  + Free Software for extracting Microsoft cabinet files, also called .CAB files. cabextract is distributed under the GPL license. It is based on the portable LGPL libmspack library. cabextract supports all special features and all compression formats of Microsoft cabinet files.
- [X] [[https://gitlab.com/cryptsetup/cryptsetup][cryptsetup]]
  + Cryptsetup and LUKS - open-source disk encryption
- [X] [[http://www.nowrap.de/flasm][flasm]]
  + free command line assembler/disassembler of Flash ActionScript bytecode.
- [X] [[http://foremost.sourceforge.net][foremost]]
  + Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files, such as those generated by dd, Safeback, Encase, etc, or directly on a drive. The headers and footers can be specified by a configuration file or you can use command line switches to specify built-in file types. These built-in types look at the data

    structures of a given file format allowing for a more reliable and
    faster recovery.
- [X] [[https://www.thc.org/thc-hydra/][hydra]]
  + THC-Hydra es un archi conocido Software que intenta crakear por
    fuerza bruta la contraseña de una cantidad impresionante de
    protocolos: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT,
    MS-SQL, MYSQL, REXEC,RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC,
    POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres,
    Teamspeak, Cisco auth, Cisco enable, AFP, LDAP2, Cisco AAA
    (incorporado en el módulo de Telnet).
- [X] [[http://packages.ubuntu.com/precise/libafflib0][libafflib0]]
  + support for Advanced Forensics format
- [X] [[http://forensicswiki.org/wiki/Libewf][libewf]]
  + Libewf is a library to access the Expert Witness Compression Format
    (EWF).

Checklist de artefactos

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../DOC_ANEXA/worg.css' />

Los principales artefactos en un sistema de ficheros con Windows 2003
instalado son:

*Ficheros de registro*

Windows define al registro como una base de datos jerárquica central
utilizada en todas las versiones de Windows, con el fin de almacenar
información necesaria para configurar el sistema para uno o varios
usuarios, aplicaciones y dispositivos hardware. El registro contiene
información que Windows utiliza como referencia constantemente, como por
ejemplo los perfiles de usuario, las aplicaciones instaladas, los
parches o HotFixes instalados, etc... Los archivos del registro de
Windows se almacenan en archivos binarios, es decir, que si abrimos
estos ficheros con un editor de texto, como puede ser notepad, no
podremos leerlo.

El registro se puede manipular desde muchos medios, tanto en línea de
```

comandos como por la propia interfaz gráfica de Windows. Evidentemente la forma más fácil de manipular el registro es de forma gráfica. Sólo tendríamos que ejecutar la herramienta ~regedit~.

El Registro está organizado en una estructura jerárquica compuesta por subárboles con sus respectivas claves, subclaves y entradas.

Las claves pueden contener subclaves y éstas, a su vez, pueden contener otras subclaves. Generalmente, la mayor parte de la información del Registro se almacena en disco y se considera permanente, aunque en determinadas circunstancias hay datos que se almacenan en claves llamadas volátiles, las cuales se sobrescriben cada vez que se inicia el sistema operativo.

Toda información relativa al sistema operativo y al PC se encuentra recogida en los archivos del sistema del registro de Windows, los cuales se localizan en %systemroot%\system32\config, y atienden a los nombres siguientes:

- /WINDOWS/system32/config/software ::
- /WINDOWS/system32/config/system ::
- /WINDOWS/system32/config/security ::
- /WINDOWS/system32/config/SAM ::
- /WINDOWS/system32/config/default ::
- /Documents\ and\ Settings/$USUARIO$/NTUSER.DAT ::
- /Documents\ and\ Settings/$USUARIO$/Local Settings/History/History.IE5/index.dat ::
- /Pagefile.sys :: El archivo de paginación es un archivo que Windows utiliza como si fuera memoria RAM (Memoria de acceso aleatorio). Este archivo esta situado en la raiz del disco duro y por defecto lo marca como oculto. El archivo de paginación y la memoria física conforman la memoria virtual. De manera predeterminada, Windows almacena el archivo de paginación en la partición de inicio, que es la partición que contiene el sistema operativo y sus archivos auxiliares. El tamaño predeterminado o recomendado del archivo de paginación es igual a 1,5 veces la cantidad total de memoria RAM.

Correspondencias:

- HKEY_USERS :: \Documents and Setting\User Profile\NTUSER.DAT
- HKEY_USERS\DEFAULT :: C:\Windows\system32\config\default
- HKEY_LOCAL_MACHINE\SAM :: C:\Windows\system32\config\SAM
- HKEY_LOCAL_MACHINE\SECURITY :: C:\Windows\system32\config\SECURITY
- HKEY_LOCAL_MACHINE\SOFTWARE :: C:\Windows\system32\config\software
- HKEY_LOCAL_MACHINE\SYSTEM :: C:\Windows\system32\config\system

Claves básicas a recuperar:

- Hora de instalación del equipo:

  + HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate

- Zona horaria:

  + HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation\StandardName
  + HKLM\SYSTEM\ControlSet001\Control\TimeZoneInformation\DaylightName

- Software instalado:

  + HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

- Tarjetas de red:

  + HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkCards\

- Paramétros de red:

  +
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

- Actualización automática de parches

  + HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU

- Profile list

  + HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

- Firewall

  +
    HKEY_LOCAL_MACHINE\RegTemp\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\

- Unidades compartidas

  +
    HKEY_LOCAL_MACHINE\\SYSTEM\CurrentControlSet\Services\LanmanServer\Shares

- URLs accedidas

  + HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

- Documentos recientes

  + NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

ficheros Log

Son una fuente de información importantísima en un análisis forense. Los sistemas Windows basados en NT tienen su principal fuente de Log en los archivos de sistema siguientes:

- SysEvent.Evt :: Registra los sucesos relativos al sistema
- SecEvent.Evt :: Registra los sucesos relativos a la seguridad
- AppEvent.Evt :: Registra los sucesos relativos a aplicaciones

Estos ficheros se encuentran en el directorio ~%systemroot%\system32\config~.

Cookies

Una cookie no es más que un fichero de texto. El funcionamiento es bastante sencillo. Algunos servidores piden a nuestro navegador que escriba en nuestro disco duro, y nuestro navegador escribe en un fichero de texto información acerca de lo que hemos estado haciendo por sus páginas. Una de las mayores ventajas de las cookies es que se almacenan en el equipo del usuario. Con esto conseguimos liberar al servidor de una sobrecarga en su espacio de disco. Cuando el servidor solicite esa información, nuestro navegador se la enviará en forma de cookie. Las cookies poseen una fecha de caducidad, que puede oscilar desde el tiempo que dure la sesión hasta una fecha especificada, a partir de la cual dejan de ser operativas. En un sistema Windows 2K/XP/2K3, las cookies se encuentran en la ruta ~C:\Documents and Settings\Nombre_Usuario\Cookies~.

En Internet Explorer existe una cookie por cada dirección de Internet que visitamos, con la nomenclatura ~Identificador_Usuario@dominio.txt~.

Para ver el contenido de una cookie, sólo tenemos que editarla con un editor de texto. Las cookies se almacenan en memoria hasta que salimos del navegador, momento en el que se escriben en el disco. Para ver las cookies que nos pide un determinado sitio Web cuando estamos conectados, podremos escribir en la barra de direcciones este simple comando:

JavaScript:alert(document.cookie);

Acto seguido nos saldrá un cuadro de alerta, con el contenido de la cookie que nos pide el servidor.

Limitaciones de las Cookies

- Trescientas cookies en total en el archivo de cookies. Si llega la número 301, se borra la más antigua.

- Veinte cookies por servidor o dominio.

- 4 Kb por cookie, para la suma del nombre y valor de la cookie.

- Ninguna máquina fuera del dominio de la cookie puede leerla.

Riesgos reales de una cookie

- Visualizar los datos contenidos en las cookies.

- Utilizar los servicios a los que permiten acceder los username y passwords almacenados en una cookie.

- Conocer las preferencias del usuario (posibilidad de envío de propaganda personalizada).

Service Pack, HotFix

Un Service Pack mantiene la versión de Windows y/o aplicaciones actualizados, corrigen problemas conocidos así como ampliar funcionalidad al equipo. En un Service Pack se incluyen drivers o controladores, herramientas y actualizaciones, así como algunas mejoras realizadas después de la puesta al público del producto. Y todo esto incluido en un paquete.

Cada nuevo Service Pack contiene todas las soluciones incluidas en los anteriores, es decir, cada Service Pack es acumulativo. Para mantener actualizado nuestro sistema sólo necesitaremos instalar el último Service Pack para cada producto o versión de Windows, ya que los Service Packs son específicos para cada producto. No se utiliza el mismo Service Pack para actualizar un Windows XP, que para actualizar un Windows 2000, por ejemplo.

Un HotFix básicamente es una revisión de un producto. Estas revisiones se realizan con el fin de subsanar errores específicos para los que no existe una solución viable.

Un HotFix no se somete a pruebas rigurosas, por lo que se recomienda aplicar estas revisiones, si se experimenta el problema exacto.

Cada cierto tiempo, al incorporarse nuevas funcionalidades y actualizaciones en los Service Packs, estos HotFix se someten a comprobaciones más exhaustivas, y se ponen a disposición del público en general.

La rama encargada de programar HotFix en Microsoft se denomina Ingeniería de corrección rápida o QFE (Quick Fix Engineering).

Proceso de análisis

El proceso de análisis es otra de las claves de la investigación informática forense, y el tiempo dedicado al mismo es crítico, ya que si no se le dedica el esfuerzo adecuado puede que no se llegue a los resultados adecuados.
En el caso de la prueba de concepto, no se ha considerado crítico la realización de un análisis exhaustivo, ya que el objetivo es analizar la viabilidad de ejecutar el mismo dentro del contexto planteado por el proyecto fin de carrera.
Por lo tanto, se van a ejecutar un número de análisis adecuado al objetivo de observar la facilidad y los problemas derivados de las limitaciones que se han impuesto en el PFC, cómo ejecutar los análisis desde Emacs, cómo trabajar y presentar los datos y como integrarlos en el informe.
El informe se ha desarrollado utilizando la técnica de `Programación Literaria` que se ha explicado en el capítulo relativo a Emacs. De este modo se puede exportar a el fichero `./4_INFORMES/poc.sh` todo el código de los comandos que se han lanzado y que no requieren de intervención manual, lo que facilita la repetición exacta de muchos de los análisis realizados.
Por otro lado, además de disponer del código org que se presenta a continuación, se puede acceder al documento de análisis en formato html y pdf.

```
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../../DOC_ANEXA/worg.css' />

* Tareas de análisis

Todas las tareas del análisis se han realizado desde Emacs. Sin embargo,
en muchos casos existen varias herramientas que permiten acceder a la
información deseada, por lo que, con el objetivo de poder disponer de
conocimientos acerca de distintas herramientas, iré utilizando varias de
ellas a pesar de que con menos herramientas también sería posible
realizar el análisis.

** Código del fichero exportado

No todos los comandos que se han ejecutado pueden exportarse
adecuadamente a un fichero de código, sin embargo se ha tratado de crear
un fichero lo más completo posible.

Para obtenerlo se debe de exportar el siguiente bloque de código (~C-c
C-v C-t~) y éste es accesible en [[./poc.sh]]:
```

```
#+NAME:crea_fichero
#+HEADERS: :shebang #!/bin/sh
#+HEADERS: :tangle ~/pfc/PoC-PFC-001/3_EVIDENCIAS/poc.sh
#+HEADERS: :mkdirp yes
#+BEGIN_SRC sh :results output :exports code :noweb yes :padline no
#
# Script de prueba de concepto
<<bulk-extractor>>
<<fsstat>>
<<montar_disco>>
<<datos_del_SSOO>>
<<zona_horaria>>
<<exporta_evt>>
<<bkhive>>
<<samdump2>>
<<john_the_ripper>>
<<john_show>>
<<software_instalado>>
<<networkcards>>
<<nic>>
<<shutdown>>
<<profilelist>>
<<firewall>>
<<shares>>
<<termserv>>
<<prefetch>>
<<mrt>>
<<samparse>>
<<samparse_tln>>
<<j_recentdocs>>
<<j_typedurls>>
<<j_IE5_index_dat>>
<<j_typedurls_tln>>
<<v_recentdocs>>
<<v_typedurls>>
<<v_IE5_index_dat>>
<<v_typedurls_tln>>
<<mac_robber>>
<<mactime>>
#+END_SRC

** Bloquear fichero windows2003.img en MacOS

En mi caso, por precaución, bloqueo el fichero desde el sistema de
ficheros MacOs que es el sistema host que soporta la máquina
virtualizada con Linux.

[[./PoC-PFC-001/3_EVIDENCIAS/bloqueo_fichero_MacOs.png]]
```

** Ejecutamos bulk-extractor

Antes de montar el fichero se analiza el mismo con ~bulk-extractor~ para obtener una serie de información genérica que posteriormente será analizada:

#+NAME:bulk-extractor
#+BEGIN_SRC sh
#Data carving
cd ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/
bulk-extractor -o output ./windows2003.img
#+END_SRC

** Identificar el tipo de sistema de ficheros de la evidencia

Al intentar editar el fichero de imagen de la máquina desde Emacs la máquina de laboratorio, incluso ampliándola a 12 Gb de RAM no logra editar el fichero en modo hexadecimal.

Para resolver el problema finalmente he instalado el paquete [[https://github.com/m00natic/v
vez ejecutado (~M-x vlf~), dado que el fichero no aparece en hexadecimal, hay que ejecutar ~hexl-mode~.

#+BEGIN_EXAMPLE
00000000: eb52 904e 5446 5320 2020 2000 0208 0000 .R.NTFS   .....
00000010: 0000 0000 00f8 0000 3f00 ff00 3f00 0000 ....?...?...
00000020: 0000 0000 8000 8000 fd25 9c00 0000 0000 ....%......
00000030: 0000 0400 0000 0000 5fc2 0900 0000 0000 ...._.......
00000040: f600 0000 0100 0000 d085 03a8 b603 a8a4 ....
00000050: 0000 0000 fa33 c08e d0bc 007c fbb8 c007 .....3.....|....
00000060: 8ed8 e816 00b8 000d 8ec0 33db c606 0e00 ....3.....
00000070: 10e8 5300 6800 0d68 6a02 cb8a 1624 00b4 ..S.h..hj....$..
00000080: 08cd 1373 05b9 ffff 8af1 660f b6c6 4066 ...s......f...@f
00000090: 0fb6 d180 e23f f7e2 86cd c0ed 0641 660f .....?.......Af.
000000a0: b7c9 66f7 e166 a320 00c3 b441 bbaa 558a ..f..f. ...A..U.
000000b0: 1624 00cd 1372 0f81 fb55 aa75 09f6 c101 .$...r...U.u....
000000c0: 7404 fe06 1400 c366 601e 0666 a110 0066 t......f`..f...f
000000d0: 0306 1c00 663b 0620 000f 823a 001e 666a ....f;. ...:..fj
000000e0: 0066 5006 5366 6810 0001 0080 3e14 0000 .fP.Sfh.....>...
000000f0: 0f85 0c00 e8b3 ff80 3e14 0000 0f84 6100 ....>.....a.
00000100: b442 8a16 2400 161f 8bf4 cd13 6658 5b07 .B..$.......fX[.
00000110: 6658 6658 1feb 2d66 33d2 660f b70e 1800 fXfX..-f3.f.....
00000120: 66f7 f1fe c28a ca66 8bd0 66c1 ea10 f736 f......f..f....6
00000130: 1a00 86d6 8a16 2400 8ae8 c0e4 060a ccb8 ......$.........
00000140: 0102 cd13 0f82 1900 8cc0 0520 008e c066 ....f
00000150: ff06 1000 ff0e 0e00 0f85 6fff 071f 6661 ....o...fa
00000160: c3a0 f801 e809 00a0 fb01 e803 00fb ebfe ....
00000170: b401 8bf0 ac3c 0074 09b4 0ebb 0700 cd10 .....<.t........
00000180: ebf2 c30d 0a41 2064 6973 6b20 7265 6164 .....A disk read

```
00000190: 2065 7272 6f72 206f 6363 7572 7265 6400   error occurred.
000001a0: 0d0a 4e54 4c44 5220 6973 206d 6973 7369  ..NTLDR is missi
000001b0: 6e67 000d 0a4e 544c 4452 2069 7320 636f  ng...NTLDR is co
000001c0: 6d70 7265 7373 6564 000d 0a50 7265 7373  mpressed...Press
000001d0: 2043 7472 6c2b 416c 742b 4465 6c20 746f   Ctrl+Alt+Del to
000001e0: 2072 6573 7461 7274 0d0a 0000 0000 0000   restart........
000001f0: 0000 0000 0000 0000 83a0 b3c9 0000 55aa  ..............U.
00000200: 0500 4e00 5400 4c00 4400 5200 0400 2400  ..N.T.L.D.R...$.
00000210: 4900 3300 3000 00e0 0000 0030 0000 0000  I.3.0......0....
#+END_EXAMPLE
```

Mirando los primeros bytes con un editor hexadecimal puede verse que corresponde a la cabecera de un sistema de ficheros NTFS.

No me planteo arrancar el sistema por el propio planteamiento del PFC de utilizar exclusivamente Emacs. Sin embargo, de ser necesario por alguna razón, se podría realizar utilizando un despliegue con [[https://www.vagrantup.com][Vagrant]] y t analizar los puertos intentar acceder al sistema.

Por otro lado, podemos realizar un doble chequeo y verificamos paralelamente que el sistema de ficheros es NTFS como se observa de la salida del comando [[http://www.sleuthkit.org/sleuthkit/man/fsstat.html][fsstat]].

```
#+NAME:fsstat
#+BEGIN_SRC sh
#Información del sistema de ficheros
fsstat ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/windows2003.img
#+END_SRC

#+BEGIN_EXAMPLE
FILE SYSTEM INFORMATION
--------------------------------------------
File System Type: NTFS
Volume Serial Number: A4A803B6A80385D0
OEM Name: NTFS
Version: Windows XP

METADATA INFORMATION
--------------------------------------------
First Cluster of MFT: 262144
First Cluster of MFT Mirror: 639583
Size of MFT Entries: 1024 bytes
Size of Index Records: 4096 bytes
Range: 0 - 19632
Root Directory: 5

CONTENT INFORMATION
--------------------------------------------
Sector Size: 512
```

```
Cluster Size: 4096
Total Cluster Range: 0 - 1279166
Total Sector Range: 0 - 10233340

$AttrDef Attribute Values:
$STANDARD_INFORMATION (16)   Size: 48-72   Flags: Resident
$ATTRIBUTE_LIST (32)   Size: No Limit   Flags: Non-resident
$FILE_NAME (48)   Size: 68-578   Flags: Resident,Index
$OBJECT_ID (64)   Size: 0-256   Flags: Resident
$SECURITY_DESCRIPTOR (80)   Size: No Limit   Flags: Non-resident
$VOLUME_NAME (96)   Size: 2-256   Flags: Resident
$VOLUME_INFORMATION (112)   Size: 12-12   Flags: Resident
$DATA (128)   Size: No Limit   Flags:
$INDEX_ROOT (144)   Size: No Limit   Flags: Resident
$INDEX_ALLOCATION (160)   Size: No Limit   Flags: Non-resident
$BITMAP (176)   Size: No Limit   Flags: Non-resident
$REPARSE_POINT (192)   Size: 0-16384   Flags: Non-resident
$EA_INFORMATION (208)   Size: 8-8   Flags: Resident
$EA (224)   Size: 0-65536   Flags:
$LOGGED_UTILITY_STREAM (256)   Size: 0-65536   Flags: Non-resident
~ $
#+END_EXAMPLE

** [[http://forensicswiki.org/wiki/Mounting_Disk_Images][Montar el fichero]] windows2003.img

Una vez conocido el sistema de ficheros se monta el fichero ~img~ para
acceder a los ficheros que contiene:

,+NAME:montar_disco
,+BEGIN_SRC sh
, Montar la imagen de disco
sudo kpartx -v -a windows2003.img
sudo mount /dev/loop0 /media/investigador/ -o -ro
#+END_SRC

#+BEGIN_EXAMPLE
Welcome to the Emacs shell

~ $ sudo kpartx -v -a ~/Escritorio/pfc/PoC-PFC-001/windows2003.img
failed to stat() /home/investigador/Escritorio/pfc/PoC-PFC-001/windows2003.img
~ $ sudo kpartx -v -a ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/windows2003.img
device-mapper: resume ioctl on loop0p1 failed: Invalid argument
create/reload failed on loop0p1
add map loop0p1 (0:0): 0 1701990410 linear /dev/loop0 218129509
device-mapper: resume ioctl on loop0p2 failed: Invalid argument
create/reload failed on loop0p2
add map loop0p2 (0:0): 0 543974724 linear /dev/loop0 729050177
device-mapper: resume ioctl on loop0p4 failed: Invalid argument
create/reload failed on loop0p4
```

```
add map loop0p4 (0:0): 0 51635 linear /dev/loop0 2692939776
~ $ sudo mount /dev/loop0 /media/investigador/ -o -ro
#+END_EXAMPLE
```

** Fecha instalación del equipo

El resultado obtenido tras acceder a ~Microsoft\Windows NT\CurrentVersion~ y listar las claves, se observa el valor de la clave ~InstallDate~:

```
#+BEGIN_EXAMPLE
4  REG_DWORD         <InstallDate>     1138258604 [0x43d872ac]
#+END_EXAMPLE
```

El dato facilitado son los segundos transcurridos desde el 1 de enero de 1970, y para conocer la fecha y hora concreta debe de realizarse el correspondiente cálculo.

Sumando 1138258604 segundos al 1/1/1970 obtenemos ~Thu, 26 Jan 2006 06:56:44 GMT~.

El cálculo se puede realizar aplicando el siguiente [[http://www.onlineconversion.com/unix_time.h

```
#+BEGIN_SRC javascript
function timeToHuman()
  {
    var theDate = new Date(document.u2h.timeStamp.value * 1000);
    dateString = theDate.toGMTString();
document.u2h.result.value = dateString;
  }
#+END_SRC
```

** Sistema operativo

Se accede a los ficheros contenidos en ~\Windows\System32\Config~ con el objetivo de obtener, mediante ~chntpw~, los datos del sistema operativo instalado:

```
#+NAME:datos_del_SSOO
#+BEGIN_SRC sh
#Obtener datos acerca del SSOO a partir del registro
cd /media/investigador/WINDOWS/system32/config
chntpw -i software
#+END_SRC
```

Los resultados obtenidos son:

```
#+BEGIN_EXAMPLE
> cat Microsoft\Windows NT\CurrentVersion\ProductName
```

```
Value <Microsoft\Windows NT\CurrentVersion\ProductName> of type REG_SZ, data length 66 [0x42
Microsoft Windows Server 2003 R2

> cat Microsoft\Windows NT\CurrentVersion\CSDVersion
Value <Microsoft\Windows NT\CurrentVersion\CSDVersion> of type REG_SZ, data length 30 [0x1e]
Service Pack 1
#+END_EXAMPLE
```

El ~Product Key~ con el que fué instalado se obtiene directamente:

```
#+BEGIN_EXAMPLE
Loaded hives: <SAM> <SECURITY> <default> <software> <userdiff> <system>

  1 - Edit user data and passwords
  3 - RecoveryConsole settings
  4 - Show product key (DigitalProductID)
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)


What to do? [1] -> 4
Value <\Microsoft\Windows NT\CurrentVersion\DigitalProductId> of type REG_BINARY, data lengt

Decoded product ID: [CCK3GXQV9G4JF223WF7PDQC6Y]
#+END_EXAMPLE
```

** Zona horaria

```
#+NAME:zona_horaria
#+BEGIN_SRC src
#Configuración de la zona horaria
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p timezone
#+END_SRC
```

Hay varias opciones para obtener los datos referentes a la zona horaria:

```
#+BEGIN_EXAMPLE
Launching timezone v.20130830
timezone v.20130830
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time Thu Feb  2 01:39:50 2006 (UTC)
  DaylightName   -> Pacific Daylight Time
  StandardName   -> Pacific Standard Time
  Bias           -> 480 (8 hours)
```

```
  ActiveTimeBias -> 480 (8 hours)
#+END_EXAMPLE

O podemos utilizar ~chntpw~:

#+BEGIN_EXAMPLE
> cat ControlSet001\Control\TimeZoneInformation\StandardName
Value <ControlSet001\Control\TimeZoneInformation\StandardName> of type REG_SZ, data length 44 [0x
Pacific Standard Time


> cat ControlSet001\Control\TimeZoneInformation\DaylightName
Value <ControlSet001\Control\TimeZoneInformation\DaylightName> of type REG_SZ, data length 44 [0x
Pacific Daylight Time
#+END_EXAMPLE

** Exportación de ficheros ~evt~

Utilizando la herramienta ~[[http://manned.org/evtexport/7573a4f8][evtexport]]~ se obtiene el con
ficheros:

- AppEvent.Evt
- SecEvent.Evt
- DnsEvent.Evt
- SysEvent.Evt

#+NAME:exporta_evt
#+BEGIN_SRC sh
#Exporta los eventos del sistema
evtexport -m all -p /media/investigador/ -r ./ -t system ./SysEvent.Evt|tee ~/Escritorio/pfc/PoC-
evtexport -m all -p /media/investigador/ -r ./ -t application ./AppEvent.Evt|tee ~/Escritorio/pfc
evtexport -m all -p /media/investigador/ -r ./ -t security ./SecEvent.Evt|tee ~/Escritorio/pfc/Po
evtexport -m all -p /media/investigador/ -r ./ ./DnsEvent.Evt|tee ~/Escritorio/pfc/PoC-PFC-001/3_
#+END_SRC

** Obtener listado de usuarios

#+BEGIN_EXAMPLE
Loaded hives: <SAM><software>

  1 - Edit user data and passwords
  3 - RecoveryConsole settings
  4 - Show product key (DigitalProductID)
      - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)


What to do? [1] -> 1
```

```
===== chntpw Edit User Info & Passwords ====

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                  | ADMIN  |          |
| 03f0 | amado                          |        |          |
| 03f7 | caracheo                       |        |          |
| 03ef | ernesto                        | ADMIN  |          |
| 01f5 | Guest                          |        | dis/lock |
| 03ee | Johnatan                       | ADMIN  |          |
| 03f6 | katy                           |        |          |
| 03f2 | lalo                           |        |          |
| 03f1 | maick                          |        |          |
| 03f4 | maru                           | ADMIN  |          |
| 03f5 | mirna                          |        |          |
| 03f3 | moni                           |        |          |
| 03fc | mpenelope                      |        | dis/lock |
| 03f8 | ovejas                         |        |          |
| 03fa | pili                           |        |          |
| 03ff | postgres                       |        |          |
| 03f9 | reno                           |        |          |
| 03e9 | SUPPORT_388945a0               |        | dis/lock |
| 0400 | ver0k                          | ADMIN  |          |
| 03fb | zamorano                       |        |          |

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !
```

#+END_EXAMPLE

** Obtener las contraseñas

Para obtener el fichero con los hashes de los usuarios (de la [[https://en.wikipedia.org/wik
que obtener el Syskey ([[https://en.wikipedia.org/wiki/Syskey][System key]]), y finalmente c
para determinar las contraseñas de los usuarios.

Los comandos utilizados, así como los resultados son:

#+NAME:bkhive
#+BEGIN_SRC src
#Obtenemos el Syskey con bkhive
cd /media/investigador/WINDOWS/system32/config/
bkhive system ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/hive.txt
#+END_SRC

#+BEGIN_EXAMPLE
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch

```
original author: ncuomo@studenti.unina.it

Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: a116697256def38326a4f58e1197c553
#+END_EXAMPLE

#+NAME:samdump2
#+BEGIN_SRC src
#Obtenemos los hashes
cd /media/investigador/WINDOWS/system32/config/
samdump2 SAM ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/hive.txt > ~/Escritorio/pfc/PoC-PFC-001/3_
#+END_SRC

Una vez obtenido el fichero con los hashes, utilizamos John the ripper
para obtener las contraseñas, como se puede ver a continuación:

#+NAME:john_the_ripper
#+BEGIN_SRC src
#craqueo de contraseñas
john ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/hash.txt
#+END_SRC

#+BEGIN_EXAMPLE
Loaded 37 password hashes with no different salts (LM [DES 128/128 SSE2-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
MORA             (zamorano:2)
P0STGR3          (postgres:1)
R3N0             (reno:2)
PASSWOR          (ver0k:1)
                 (SUPPORT_388945a0)
                 (Guest)
1                (mpenelope:2)
2000             (moni:2)
CARMEN8          (amado:1)
D                (ver0k:2)
4                (lalo:2)
R                (ernesto:2)
LY               (pili:2)
3                (mirna:2)
3                (amado:2)
18               (maick:2)
JUANG11          (maick:1)
MELUCHA          (maru:1)
30               (caracheo:2)
83               (katy:2)
RODOLFO          (reno:1)
MMONICA          (moni:1)
026              (maru:2)
```

```
LALOLOC          (ovejas:1)
O86              (ovejas:2)
TEGUIZA          (zamorano:1)
CHIRIPI          (pili:1)
CHLN026          (katy:1)
MIRK4AR          (mirna:1)
T3R3CLT          (lalo:1)
T3MP0RA          (mpenelope:1)
T3WPJ0H          (Johnatan)
SSQL             (postgres:2)
3RN3S70          (ernesto:1)
L,               (Administrator:2)
U7R3$7U          (Administrator:1)
C4R$4CH          (caracheo:1)
37g 0:02:51:36 3/3 0.003593g/s 45521Kp/s 45521Kc/s 90542KC/s C4R$4BU..C4R$4DW
Warning: passwords printed above might be partial
Use the '--show' option to display all of the cracked passwords reliably
Session completed
~ $
#+END_EXAMPLE
```

A continuación se presenta un listado con el formato
~USUARIO:CONTRASEÑA:ID:resto~

```
#+NAME:john_show
#+BEGIN_SRC src
#Obtenemos el listado de usuarios y contraseñas
investigador@EFI:~/Escritorio$ john --show hash.txt
#+END_SRC

#+BEGIN_EXAMPLE
Administrator:U7R3$7UL,:500:fad82559a3669bf1c349641028e9bf3b:ecde6a92576ca84b5ddcd7cb117bab5
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0::1001:aad3b435b51404eeaad3b435b51404ee:8dcca3eb5e2ed3503e483df0dce5f072:::
Johnatan:T3WPJ0H:1006:fbc89204579fc565aad3b435b51404ee:7750def414475cf2b9b45a64fdd3481a:::
ernesto:3RN3S70R:1007:aa4d59741693011a944e2df489a880e4:2c759a0f3165fe70f3b2ef1355dbbf4e:::
amado:CARMEN83:1008:59cbc5117eaef5c21aa818381e4e281b:0ade3431a00b403ccc562b6cf629ab77:::
maick:JUANG1118:1009:85fec305e34929d18347bb1e72cc9f76:0e13f8a840ea89fcd88cb36b962a2f14:::
lalo:T3R3CLT4:1010:3264cf6b06490f7cff17365faf1ffe89:10ee4264b00cc787b80f6f3c80dcf9c5:::
moni:MMONICA2000:1011:506b60f26bb9aeef8b4c5fc57ce52905:0ac8ae6ef8beaae7c61cf4230c7a3b8d:::
maru:MELUCHA026:1012:03fb789ef35a2b6d40967f66e935e1ff:2e4f31fe3248f2bc9d1e961b579f0e5f:::
mirna:MIRK4AR3:1013:4547b34ebb1a63e81aa818381e4e281b:b84ef18830b2b30ba60105d507eaaec9:::
katy:CHLN02683:1014:b487217fce8da54ddc0adaac127d3673:2ce609fe8387032f3c7fbbfc7f4bd931:::
caracheo:C4R$4CH30:1015:10972d878c8158d23830ab41f50b8c79:1f29efc37cc7c33148c3b1a16b81c45e:::
ovejas:LALOLOCO86:1016:36cea0da9720c1866f3baf47315038ff:16fb5c5803db901b39f38adcfda64bf7:::
reno:RODOLFOR3N0:1017:f903d899f9f2f54138e225910e5ac3d2:da8ffa76f679c3a79d46b96d61758f34:::
pili:CHIRIPILY:1018:7ed41ffdc962e828527c3e14a6132a0f:8963676b5ef71347321fca96dfcf2243:::
zamorano:TEGUIZAMORA:1019:4f11278e04ff02b3451e935871f3e930:5550a4a120a88cfc12e1c856344d93c6:
mpenelope:T3MP0RA1:1020:7d536e187e4a5a05c2265b23734e0dac:2a6f455e8094160b511a810e4e8aee61:::
```

```
postgres:P0STGR3SSQL:1023:c848af05f3d8ca3c929ca03322bf4367:6812a8dcfcad8c09a65696fa3e893d31:::
ver0k:PASSWORD:1024:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::

37 password hashes cracked, 0 left
#+END_EXAMPLE

** Software Instalado

El software instalado en el equipo es:

#+NAME:software_instalado
#+BEGIN_SRC src
#Obtenemos el listado de software instalado
cd /media/investigador/WINDOWS/system32/config/
sudo perl /usr/share/regripper/rip.pl -r software -p uninstall
#+END_SRC

#+BEGIN_EXAMPLE
Launching uninstall v.20140512
uninstall v.20140512
(Software, NTUSER.DAT) Gets contents of Uninstall keys from Software, NTUSER.DAT hives

Uninstall
Microsoft\Windows\CurrentVersion\Uninstall

Sun Feb  5 21:14:35 2006 (UTC)
  MPlayer2

Sat Feb  4 22:46:58 2006 (UTC)
  PostgreSQL 8.1 v.8.1

Sat Feb  4 02:05:29 2006 (UTC)
  MSN Messenger 7.5 v.7.5.0311.0

Sat Feb  4 01:52:54 2006 (UTC)
  Mozilla Firefox (1.5.0.1) v.1.5.0.1 (es-ES)

Fri Jan 27 02:43:01 2006 (UTC)
  MySQL Administrator 1.1 v.1.1.7

Fri Jan 27 02:39:50 2006 (UTC)
  MySQL Server 4.1 v.4.1.16

Fri Jan 27 02:04:01 2006 (UTC)
  PHP 4.4.2

Fri Jan 27 02:00:42 2006 (UTC)
  Apache HTTP Server 1.3.34 v.1.3.34
```

```
Thu Jan 26 22:02:34 2006 (UTC)
  Security Update for Windows Server 2003 (KB905414) v.1

Thu Jan 26 22:02:16 2006 (UTC)
  Security Update for Windows Server 2003 (KB890046) v.1
  Security Update for Windows Server 2003 (KB896428) v.1
  Security Update for Windows Server 2003 (KB899587) v.1

Thu Jan 26 22:00:38 2006 (UTC)
  Security Update for Windows Server 2003 (KB901017) v.1

Thu Jan 26 22:00:16 2006 (UTC)
  Security Update for Windows Server 2003 (KB899589) v.1

Thu Jan 26 21:59:39 2006 (UTC)
  Security Update for Windows Server 2003 (KB908519) v.1

Thu Jan 26 21:59:17 2006 (UTC)
  Security Update for Windows Server 2003 (KB903235) v.1

Thu Jan 26 21:58:42 2006 (UTC)
  Security Update for Windows Server 2003 (KB901214) v.1
  Security Update for Windows Server 2003 (KB902400) v.1

Thu Jan 26 21:56:03 2006 (UTC)
  Update for Windows Server 2003 (KB896727) v.1

Thu Jan 26 21:55:11 2006 (UTC)
  Security Update for Windows Server 2003 (KB896688) v.1

Thu Jan 26 21:54:22 2006 (UTC)
  Security Update for Windows Server 2003 (KB896358) v.20050421.234609
  Security Update for Windows Server 2003 (KB896422) v.1
  Security Update for Windows Server 2003 (KB896424) v.1

Thu Jan 26 06:42:36 2006 (UTC)
  DXM_Runtime

Thu Jan 26 06:42:12 2006 (UTC)
  Branding

Thu Jan 26 06:39:34 2006 (UTC)
  PCHealth

Thu Jan 26 06:39:31 2006 (UTC)
  AddressBook
  DirectAnimation
  NetMeeting
  OutlookExpress
```

```
Thu Jan 26 06:39:30 2006 (UTC)
  ICW

Thu Jan 26 06:39:25 2006 (UTC)
  DirectDrawEx
  Fontcore
  IE40
  IE4Data
  IE5BAKEX
  IEData
  MobileOptionPack
  SchedulingAgent

Thu Jan 26 06:26:49 2006 (UTC)
  Connection Manager

/media/investigador/WINDOWS/system32/config $
#+END_EXAMPLE
```

** Información sobre las tarjetas de red

Se observa que hay dos tarjetas instaladas desde el día de inicial.

```
#+NAME:networkcards
#+BEGIN_SRC src
#Obtenemos el listado de tarjetas de red
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r software -p networkcards
#+END_SRC

#+BEGIN_EXAMPLE
Launching networkcards v.20080325
networkcards v.20080325
(Software) Get NetworkCards

NetworkCards
Microsoft\Windows NT\CurrentVersion\NetworkCards

Realtek RTL8139 Family PCI Fast Ethernet NIC  [Wed Jan 25 21:07:08 2006]
3Com 3C900B-TPO Ethernet Adapter (Generic)  [Wed Jan 25 21:07:13 2006]
#+END_EXAMPLE
```

** Información de la configuración de red

Se observa que la dirección IP es fija y no está configurado el DHCP.

```
#+NAME:nic
#+BEGIN_SRC src
```

```
#Obtenemos la configuración de networking
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p nic
#+END_SRC

#+BEGIN_EXAMPLE
/media/investigador/WINDOWS/system32/config $
Launching nic v.20100401
nic v.20100401
(System) Gets NIC info from System hive

Adapter: {44C3A521-98D1-4B7A-850D-860BB2324A1D}
LastWrite Time: Thu Jan 26 06:26:22 2006 Z
  EnableDHCP           1
  IPAddress            0.0.0.0
  SubnetMask           0.0.0.0
  DefaultGateway

Adapter: {5269ADEB-9E6D-4673-B898-4238F085972C}
LastWrite Time: Thu Jan 26 06:26:22 2006 Z
  EnableDHCP           0
  IPAddress            192.168.5.5
  SubnetMask           255.255.255.0
  DefaultGateway       192.168.5.254
  DhcpIPAddress        0.0.0.0
  DhcpSubnetMask       255.0.0.0
  DhcpServer           255.255.255.255
  Lease                3600
  LeaseObtainedTime    Sun Jan 29 01:18:17 2006 Z
  T1                   Sun Jan 29 01:48:17 2006 Z
  T2                   Sun Jan 29 02:10:47 2006 Z
  LeaseTerminatesTime  Sun Jan 29 02:18:17 2006 Z
#+END_EXAMPLE

** Fecha y hora del último apagado

Se obtiene el momento del apagado definitivo del sistema, que es un dato
necesario para el timeline.

#+NAME:shutdown
#+BEGIN_SRC src
# Obtenemos el momento del apagado
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p shutdown
#+END_SRC

#+BEGIN_EXAMPLE
Launching shutdown v.20080324
shutdown v.20080324
```

```
(System) Gets ShutdownTime value from System hive

ControlSet001\Control\Windows key, ShutdownTime value
ControlSet001\Control\Windows
LastWrite Time Sun Feb  5 23:44:32 2006 (UTC)
  ShutdownTime = Sun Feb  5 23:44:32 2006 (UTC)
#+END_EXAMPLE
```

** Profile

Aquí podemos ver que no todos los perfiles de usuario han estado activos hasta el momento del apagado del sistema, y de echo algunos apenas han tenido actividad desde el momento de su creación, por lo que se puede descartar a la hora del análisis.

Los usuarios activos en los momentos previos al apagado son, ~Johnatan~, ~ver0k~ y ~Administrator~.

```
#+NAME:profilelist
#+BEGIN_SRC src
# Obtenemos el profile
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r software -p profilelist
#+END_SRC

#+BEGIN_EXAMPLE
Launching profilelist v.20100219
profilelist v.20100219
(Software) Get content of ProfileList key

Microsoft\Windows NT\CurrentVersion\ProfileList
LastWrite Time Sun Feb  5 20:47:22 2006 (UTC)

Path      : %systemroot%\system32\config\systemprofile
SID       : S-1-5-18
LastWrite : Thu Jan 26 06:56:44 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\LocalService
SID       : S-1-5-19
LastWrite : Sat Feb  4 01:40:01 2006 (UTC)
LoadTime  : Sat Feb  4 01:39:42 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\NetworkService
SID       : S-1-5-20
LastWrite : Sun Feb  5 23:44:28 2006 (UTC)
LoadTime  : Sat Feb  4 01:39:41 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\Johnatan
SID       : S-1-5-21-2780117151-1340924567-2512508698-1006
```

```
LastWrite : Sun Feb  5 22:28:40 2006 (UTC)
LoadTime  : Sun Feb  5 20:23:09 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\maick
SID       : S-1-5-21-2780117151-1340924567-2512508698-1009
LastWrite : Sat Feb  4 03:33:37 2006 (UTC)
LoadTime  : Sat Feb  4 02:11:06 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\maru
SID       : S-1-5-21-2780117151-1340924567-2512508698-1012
LastWrite : Fri Jan 27 01:57:00 2006 (UTC)
LoadTime  : Thu Jan 26 22:59:32 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\reno
SID       : S-1-5-21-2780117151-1340924567-2512508698-1017
LastWrite : Fri Feb  3 04:38:22 2006 (UTC)
LoadTime  : Fri Feb  3 02:34:19 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\postgres
SID       : S-1-5-21-2780117151-1340924567-2512508698-1023
LastWrite : Sat Feb  4 22:46:51 2006 (UTC)
LoadTime  : Sat Feb  4 22:46:51 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\ver0k
SID       : S-1-5-21-2780117151-1340924567-2512508698-1024
LastWrite : Sun Feb  5 23:44:11 2006 (UTC)
LoadTime  : Sun Feb  5 20:47:24 2006 (UTC)

Path      : %SystemDrive%\Documents and Settings\Administrator
SID       : S-1-5-21-2780117151-1340924567-2512508698-500
LastWrite : Sun Feb  5 23:44:00 2006 (UTC)
LoadTime  : Sun Feb  5 22:29:16 2006 (UTC)

Domain Accounts
#+END_EXAMPLE

** Configuración del firewall

#+NAME:firewall
#+BEGIN_SRC src
# Configuración del firewall
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p fw_config
#+END_SRC

Podemos ver que el firewall del servidor está activo, y los puertos
abiertos (y no nateados) son:

- 445:TCP -> 445:TCP
```

```
- 2869:TCP -> 2869:TCP
- 5432:TCP -> 5432:TCP
- 138:UDP -> 138:UDP
- 139:TCP -> 139:TCP
- 3389:TCP -> 3389:TCP
- 137:UDP -> 137:UDP
- 1900:UDP -> 1900:UDP

#+BEGIN_EXAMPLE
Launching fw_config v.20080328
fw_config v.20080328
(System) Gets the Windows Firewall config from the System hive

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile
LastWrite Time Sat Feb  4 02:05:32 2006 (UTC)
EnableFirewall -> 0

ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile\AuthorizedApplication
LastWrite Time Sat Feb  4 02:05:32 2006 (UTC)
C:\Program Files\MSN Messenger\msnmsgr.exe -> C:\Program Files\MSN Messenger\msnmsgr.exe:*:Enable

Windows Firewall Configuration
ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
LastWrite Time Fri Jan 27 02:13:41 2006 (UTC)
EnableFirewall -> 1
DoNotAllowExceptions -> 0
DisableNotifications -> 0

ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\GloballyOpenPorts\L
LastWrite Time Sat Feb  4 22:49:37 2006 (UTC)
445:TCP -> 445:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22005
2869:TCP -> 2869:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22008
5432:TCP -> 5432:TCP:*:Enabled:postgrest
138:UDP -> 138:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22002
139:TCP -> 139:TCP:LocalSubNet:Enabled:@xpsp2res.dll,-22004
3389:TCP -> 3389:TCP:*:Enabled:@xpsp2res.dll,-22009
137:UDP -> 137:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22001
1900:UDP -> 1900:UDP:LocalSubNet:Enabled:@xpsp2res.dll,-22007

ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplicati
LastWrite Time Sat Feb  4 02:05:32 2006 (UTC)
C:\Program Files\BitTorrent\bittorrent.exe -> C:\Program Files\BitTorrent\bittorrent.exe:*:Enable
C:\Program Files\MSN Messenger\msnmsgr.exe -> C:\Program Files\MSN Messenger\msnmsgr.exe:*:Enable
C:\apache\Apache\Apache.exe -> C:\apache\Apache\Apache.exe:*:Enabled:Apache
#+END_EXAMPLE

** Unidades compartidas
```

No existen unidades compartidas.

```
#+NAME:shares
#+BEGIN_SRC src
# Obtenemos el listado de unidades compartidas
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p shares
#+END_SRC

#+BEGIN_EXAMPLE
Launching shares v.20140730
shares v.20140730
(System) Get list of shares from System hive file

ControlSet001\Services\lanmanserver\Shares has no values.
  NullSessionShares = COMCFG DFS$
#+END_EXAMPLE
```

** Terminal Server

Obtenemos la configuración de ~Terminal Server~ ya que es un punto de riesgo importante. Sin embargo no se ve nada inusual.

```
#+NAME:termserv
#+BEGIN_SRC src
# Obtenemos la configuración de Terminal Server
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p termserv
#+END_SRC

#+BEGIN_EXAMPLE
Launching termserv v.20130307
ControlSet001\Control\Terminal Server
LastWrite Time Sun Feb  5 20:46:23 2006 (UTC)

Reference: http://support.microsoft.com/kb/243215

  ProductVersion = 5.2

  fDenyTSConnections = 0
  1 = connections denied


  TSAdvertise = 0
  0 = disabled, 1 = enabled (advertise Terminal Services)
  Ref: http://support.microsoft.com/kb/281307

  TSEnabled = 1
  0 = disabled, 1 = enabled (Terminal Services enabled)
```

```
  Ref: http://support.microsoft.com/kb/222992

  TSUserEnabled = 0
  1 = All users logging in are automatically part of the
  built-in Terminal Server User group. 0 = No one is a
  member of the built-in group.
  Ref: http://support.microsoft.com/kb/238965

  fAllowToGetHelp = 0
  1 = Users can request assistance from friend or a
  support professional.
  Ref: http://www.pctools.com/guides/registry/detail/1213/
AutoStart Locations
Wds\rdpwd key
  StartupPrograms: rdpclip
Analysis Tip: This value usually contains 'rdpclip'; any additional entries
should be investigated.

WinStations\RDP-Tcp key
  InitialProgram: {blank}
Analysis Tip: Maybe be empty; appears as '{blank}'

UserAuthentication value not found.
#+END_EXAMPLE

** Configuración de prefetch

Verificamos que la configuración de prefetch sea correcta, y que no haya
modificaciones que puedan afectar al correcto funcionamiento del sistema
tras el reinicio del mismo.

#+NAME:prefetch
#+BEGIN_SRC src
# Obtenemos la configuración de prefetch
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r system -p prefetch
#+END_SRC

#+BEGIN_EXAMPLE
Launching prefetch v.20120914
prefetch v.20120914
(SYSTEM) Gets the the Prefetch Parameters

EnablePrefetcher    = 2

0 = Prefetching is disabled
1 = Application prefetching is enabled
2 = Boot prefetching is enabled
3 = Both boot and application prefetching is enabled
```

#+END_EXAMPLE

** Malicious Software Removal Tool

Se verifica que no se ha activado el ~Malicious Software Removal Tool~.

#+NAME:mrt
#+BEGIN_SRC src
Malicious Software Removal Tool
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r software -p mrt
#+END_SRC

#+BEGIN_EXAMPLE
Launching mrt v.20080804
mrt v.20080804
(Software) Check to see if Malicious Software Removal Tool has been run

Microsoft\RemovalTools\MRT not found.
Microsoft\RemovalTools\MRT not found.
#+END_EXAMPLE

** Información de usuarios y grupos del sistema

Aquí obtenemos información adicional que es interesante, como el número de veces que los usuarios han accedido al sistema y que nos permite descartar a muchos usuarios.

Por otro lado, el usuario ~ver0k~ es el único que apenas está documentado. No tiene nombre ni descripción y fué creado el mismo día que se apaga el servidor, pero unas horas antes, lo que implica que es un vector de investigación muy claro.

#+NAME:samparse
#+BEGIN_SRC src
Obtenemos la configuración de prefetch
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r SAM -p samparse
#+END_SRC

#+BEGIN_EXAMPLE
Launching samparse v.20120722
samparse v.20120722
(SAM) Parse SAM file for user & group mbrshp info

User Information

Username   : Administrator [500]

```
Full Name       :
User Comment    : Built-in account for administering the computer/domain
Account Type    : Default Admin User
Account Created : Wed Jan 25 21:03:58 2006 Z
Last Login Date : Sun Feb  5 22:29:16 2006 Z
Pwd Reset Date  : Wed Jan 25 21:25:43 2006 Z
Pwd Fail Date   : Fri Feb  3 04:37:46 2006 Z
Login Count     : 39
  --> Password does not expire
  --> Normal user account

Username        : Guest [501]
Full Name       :
User Comment    : Built-in account for guest access to the computer/domain
Account Type    : Default Guest Acct
Account Created : Wed Jan 25 21:03:58 2006 Z
Last Login Date : Never
Pwd Reset Date  : Never
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
  --> Account Disabled
  --> Password not required

Username        : SUPPORT_388945a0 [1001]
Full Name       : CN=Microsoft Corporation,L=Redmond,S=Washington,C=US
User Comment    : This is a vendor's account for the Help and Support Service
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 06:41:13 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 06:41:13 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Password does not expire
  --> Normal user account
  --> Account Disabled

Username        : Johnatan [1006]
Full Name       : Johnatan Tezcatlipoca
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Jan 26 22:17:06 2006 Z
Last Login Date : Sun Feb  5 20:23:09 2006 Z
Pwd Reset Date  : Mon Jan 30 21:32:56 2006 Z
Pwd Fail Date   : Sat Feb  4 03:32:24 2006 Z
Login Count     : 7
  --> Normal user account
```

```
Username        : ernesto [1007]
Full Name       : Ernesto Sánchez
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Jan 26 22:20:47 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:38:33 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : amado [1008]
Full Name       : Amado Carrillo
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:21:52 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:35:34 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : maick [1009]
Full Name       : Gabriel Torres
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:22:34 2006 Z
Last Login Date : Sat Feb  4 02:11:04 2006 Z
Pwd Reset Date  : Thu Jan 26 22:42:26 2006 Z
Pwd Fail Date   : Never
Login Count     : 1
  --> Normal user account

Username        : lalo [1010]
Full Name       : Eduardo Hernández
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:23:30 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:41:38 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : moni [1011]
Full Name       : Monica Islas
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:24:11 2006 Z
```

```
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:45:08 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : maru [1012]
Full Name       : Maria Guadalupe Ramos
User Comment    :
Account Type    : Default Admin User
Account Created : Thu Jan 26 22:25:10 2006 Z
Last Login Date : Thu Jan 26 22:59:30 2006 Z
Pwd Reset Date  : Thu Jan 26 22:43:14 2006 Z
Pwd Fail Date   : Never
Login Count     : 1
  --> Normal user account

Username        : mirna [1013]
Full Name       : Mirna Casillas
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:25:32 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:44:15 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : katy [1014]
Full Name       : Katalina Rodriguez
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:26:10 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:40:24 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : caracheo [1015]
Full Name       : Jorge Caracheo Mota
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:26:43 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:37:03 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account
```

```
Username        : ovejas [1016]
Full Name       : Eduardo Roldán
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:27:40 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:47:01 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : reno [1017]
Full Name       : Israel Robledo Gonzáles
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:28:52 2006 Z
Last Login Date : Fri Feb  3 02:34:18 2006 Z
Pwd Reset Date  : Thu Jan 26 22:48:19 2006 Z
Pwd Fail Date   : Never
Login Count     : 1
  --> Normal user account

Username        : pili [1018]
Full Name       : Elizabet Herrera Zamora
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:29:20 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:47:39 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : zamorano [1019]
Full Name       : Rolando Zamorategui
User Comment    :
Account Type    : Custom Limited Acct
Account Created : Thu Jan 26 22:29:45 2006 Z
Last Login Date : Never
Pwd Reset Date  : Thu Jan 26 22:48:58 2006 Z
Pwd Fail Date   : Never
Login Count     : 0
  --> Normal user account

Username        : mpenelope [1020]
Full Name       : Mari Carmen Penelope
User Comment    :
Account Type    : Custom Limited Acct
```

```
Account Created : Thu Jan 26 22:30:27 2006 Z
Last Login Date : Never
Pwd Reset Date  : Sat Feb  4 23:09:27 2006 Z
Pwd Fail Date   : Sat Feb  4 23:10:54 2006 Z
Login Count     : 0
  --> Normal user account

Username        : postgres [1023]
Full Name       : postgres
User Comment    : PostgreSQL service account
Account Type    : Custom Limited Acct
Account Created : Sat Feb  4 22:46:23 2006 Z
Last Login Date : Sat Feb  4 22:46:49 2006 Z
Pwd Reset Date  : Sat Feb  4 22:46:23 2006 Z
Pwd Fail Date   : Never
Login Count     : 2
  --> Password does not expire
  --> Normal user account

Username        : ver0k [1024]
Full Name       :
User Comment    :
Account Type    : Default Admin User
Account Created : Sun Feb  5 20:45:30 2006 Z
Last Login Date : Sun Feb  5 20:47:21 2006 Z
Pwd Reset Date  : Sun Feb  5 20:45:30 2006 Z
Pwd Fail Date   : Never
Login Count     : 1
  --> Normal user account

-------------------------
Group Membership Information
-------------------------
Group Name    : Print Operators [0]
LastWrite     : Wed Jan 25 21:03:59 2006 Z
Group Comment : Members can administer domain printers
Users         : None

Group Name    : Performance Log Users [1]
LastWrite     : Wed Jan 25 21:03:59 2006 Z
Group Comment : Members of this group have remote access to schedule logging of performance count
Users :
  S-1-5-20

Group Name    : Power Users [0]
LastWrite     : Wed Jan 25 21:03:58 2006 Z
Group Comment : Power Users possess most administrative powers with some restrictions.  Thus, Pow
Users         : None
```

```
Group Name    : Guests [1]
LastWrite     : Wed Jan 25 21:03:58 2006 Z
Group Comment : Guests have the same access as members of the Users group by default, except
Users :
  S-1-5-21-2780117151-1340924567-2512508698-501

Group Name    : Users [18]
LastWrite     : Sun Feb  5 20:45:30 2006 Z
Group Comment : Users are prevented from making accidental or intentional system-wide change
Users :
  S-1-5-11
  S-1-5-21-2780117151-1340924567-2512508698-1017
  S-1-5-21-2780117151-1340924567-2512508698-1014
  S-1-5-4
  S-1-5-21-2780117151-1340924567-2512508698-1013
  S-1-5-21-2780117151-1340924567-2512508698-1010
  S-1-5-21-2780117151-1340924567-2512508698-1009
  S-1-5-21-2780117151-1340924567-2512508698-1007
  S-1-5-21-2780117151-1340924567-2512508698-1008
  S-1-5-21-2780117151-1340924567-2512508698-1018
  S-1-5-21-2780117151-1340924567-2512508698-1015
  S-1-5-21-2780117151-1340924567-2512508698-1020
  S-1-5-21-2780117151-1340924567-2512508698-1019
  S-1-5-21-2780117151-1340924567-2512508698-1024
  S-1-5-21-2780117151-1340924567-2512508698-1011
  S-1-5-21-2780117151-1340924567-2512508698-1012
  S-1-5-21-2780117151-1340924567-2512508698-1016
  S-1-5-21-2780117151-1340924567-2512508698-1006

Group Name    : Network Configuration Operators [0]
LastWrite     : Wed Jan 25 21:03:59 2006 Z
Group Comment : Members in this group can have some administrative privileges to manage conf
Users         : None

Group Name    : Remote Desktop Users [0]
LastWrite     : Wed Jan 25 21:03:59 2006 Z
Group Comment : Members in this group are granted the right to logon remotely
Users         : None

Group Name    : Backup Operators [0]
LastWrite     : Wed Jan 25 21:03:58 2006 Z
Group Comment : Backup Operators can override security restrictions for the sole purpose of
Users         : None

Group Name    : Distributed COM Users [0]
LastWrite     : Wed Jan 25 21:03:59 2006 Z
Group Comment : Members are allowed to launch, activate and use Distributed COM objects on t
Users         : None
```

```
Group Name    : Administrators [5]
LastWrite     : Sun Feb  5 20:45:53 2006 Z
Group Comment : Administrators have complete and unrestricted access to the computer/domain
Users :
  S-1-5-21-2780117151-1340924567-2512508698-1007
  S-1-5-21-2780117151-1340924567-2512508698-500
  S-1-5-21-2780117151-1340924567-2512508698-1024
  S-1-5-21-2780117151-1340924567-2512508698-1006
  S-1-5-21-2780117151-1340924567-2512508698-1012

Group Name    : Performance Monitor Users [0]
LastWrite     : Wed Jan 25 21:03:59 2006 Z
Group Comment : Members of this group have remote access to monitor this computer
Users         : None

Group Name    : Replicator [0]
LastWrite     : Wed Jan 25 21:03:58 2006 Z
Group Comment : Supports file replication in a domain
Users         : None

Analysis Tips:
 - For well-known SIDs, see http://support.microsoft.com/kb/243330
     - S-1-5-4  = Interactive
     - S-1-5-11 = Authenticated Users
 - Correlate the user SIDs to the output of the ProfileList plugin
#+END_EXAMPLE

** Análisis de tiempos en usuarios y grupos del sistema

Con el objetivo de desarrollar un TLN (Time Line analisis) lo más
concreto posible se obtienen datos relativos a eventos concretos de los
distintos usuarios, como la creación de la cuenta o el último acceso de
los usuarios.

Organizando esta información podríamos observar situaciones interesantes
a la hora de realizar el análisis como una posible relación entre la
actividad de los usuarios ~Johnatan~ y ~ver0k~.

#+NAME:samparse_tln
#+BEGIN_SRC src
# Obtenemos la configuración de prefetch
cd /media/investigador/WINDOWS/system32/config
sudo perl /usr/share/regripper/rip.pl -r SAM -p samparse
#+END_SRC

#+BEGIN_EXAMPLE
/media/investigador/WINDOWS/system32/config $ sudo perl /usr/share/regripper/rip.pl -r SAM -p sam
Launching samparse_tln v.20120827
1138223038|SAM||Administrator|Acct Created (Default Admin User)
```

```
1138224343|SAM||Administrator|Password Reset Date
1138941466|SAM||Administrator|Password Failure Date
1139178556|SAM||Administrator|Last Login (39)
1138223038|SAM||Guest|Acct Created (Default Guest Acct)
1138257673|SAM||SUPPORT_388945a0|Acct Created (Custom Limited Acct)
1138257673|SAM||SUPPORT_388945a0|Password Reset Date
1138313826|SAM||Johnatan|Acct Created (Default Admin User)
1138656776|SAM||Johnatan|Password Reset Date
1139023944|SAM||Johnatan|Password Failure Date
1139170989|SAM||Johnatan|Last Login (7)
1138314047|SAM||ernesto|Acct Created (Default Admin User)
1138315113|SAM||ernesto|Password Reset Date
1138314112|SAM||amado|Acct Created (Custom Limited Acct)
1138314934|SAM||amado|Password Reset Date
1138314154|SAM||maick|Acct Created (Custom Limited Acct)
1138315346|SAM||maick|Password Reset Date
1139019064|SAM||maick|Last Login (1)
1138314210|SAM||lalo|Acct Created (Custom Limited Acct)
1138315298|SAM||lalo|Password Reset Date
1138314251|SAM||moni|Acct Created (Custom Limited Acct)
1138315508|SAM||moni|Password Reset Date
1138314310|SAM||maru|Acct Created (Default Admin User)
1138315394|SAM||maru|Password Reset Date
1138316370|SAM||maru|Last Login (1)
1138314332|SAM||mirna|Acct Created (Custom Limited Acct)
1138315455|SAM||mirna|Password Reset Date
1138314370|SAM||katy|Acct Created (Custom Limited Acct)
1138315224|SAM||katy|Password Reset Date
1138314403|SAM||caracheo|Acct Created (Custom Limited Acct)
1138315023|SAM||caracheo|Password Reset Date
1138314460|SAM||ovejas|Acct Created (Custom Limited Acct)
1138315621|SAM||ovejas|Password Reset Date
1138314532|SAM||reno|Acct Created (Custom Limited Acct)
1138315699|SAM||reno|Password Reset Date
1138934058|SAM||reno|Last Login (1)
1138314560|SAM||pili|Acct Created (Custom Limited Acct)
1138315659|SAM||pili|Password Reset Date
1138314585|SAM||zamorano|Acct Created (Custom Limited Acct)
1138315738|SAM||zamorano|Password Reset Date
1138314627|SAM||mpenelope|Acct Created (Custom Limited Acct)
1139094567|SAM||mpenelope|Password Reset Date
1139094654|SAM||mpenelope|Password Failure Date
1139093183|SAM||postgres|Acct Created (Custom Limited Acct)
1139093183|SAM||postgres|Password Reset Date
1139093209|SAM||postgres|Last Login (2)
1139172330|SAM||ver0k|Acct Created (Default Admin User)
1139172330|SAM||ver0k|Password Reset Date
1139172441|SAM||ver0k|Last Login (1)
#+END_EXAMPLE
```

** Urls accedidas (Administrator)

Vemos que el ~Administrator~ ha accedido a google, a la unidad de disco (C:) y se ha descargado la herramienta de IM de Microsoft. Sin embargo este usuario no ha accedido con ningún usuario ya que el directorio ~C:/Documents and Settings/Administrator/Application Data/Microsoft/MSN Messenger~ aparece vacío.

```
#+NAME:j_typedurls
#+BEGIN_SRC src
# Obtenemos las URLs accedidas
cd /media/investigador/Documents and Settings/Administrator
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p typedurls
#+END_SRC

#+BEGIN_EXAMPLE
Launching typedurls v.20080324
typedurls v.20080324
(NTUSER.DAT) Returns contents of user’s TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Sat Feb  4 02:06:30 2006 (UTC)
  url1 -> http://messenger.msn.com/xp/downloadx.aspx
  url2 -> Local Disk (C:)
  url3 -> http://www.google.com/
  url4 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
#+END_EXAMPLE
```

** Documentos recientes (Johnatan)

Los documentos recientes accedidos por ~Johnatan~.

```
#+NAME:j_recentdocs
#+BEGIN_SRC src
# Obtenemos los documentos recientemente accedidos
cd /media/investigador/Documents and Settings/Johnatan
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p recentdocs
#+END_SRC

#+BEGIN_EXAMPLE
Launching recentdocs v.20100405
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user’s RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
```

```
LastWrite Time Sun Feb  5 22:21:02 2006 (UTC)
  1 = L3 (D:)
  0 = index.html

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.html
LastWrite Time Sun Feb  5 22:21:02 2006 (UTC)
MRUListEx = 0
  0 = index.html

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Sun Feb  5 22:21:02 2006 (UTC)
MRUListEx = 0
  0 = L3 (D:)
#+END_EXAMPLE
```

** Urls accedidas (Johnatan)

Vemos que ~Johnatan~ ha accedido a google, al correo de yahoo y seguidamente al ERP.

```
#+NAME:j_typedurls
#+BEGIN_SRC src
# Obtenemos las URLs accedidas
cd /media/investigador/Documents and Settings/Johnatan
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p typedurls
#+END_SRC

#+BEGIN_EXAMPLE
Launching typedurls v.20080324
typedurls v.20080324
(NTUSER.DAT) Returns contents of user’s TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Sun Feb  5 22:20:08 2006 (UTC)
  url1 -> http://127.0.0.1/web-erp
  url2 -> http://127.0.0.1/web-erp/
  url3 -> http://mail.yahoo.com/
  url4 -> http://www.google.com/
  url5 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
#+END_EXAMPLE
```

Adicionalmente de ha extraído la información del fichero index.dat de su navegación y se ha guardado como evidencia.

```
#+NAME:j_IE5_index_dat
#+BEGIN_SRC src
# Obtenemos la información de index.dat
cd /media/investigador/Documents and Settings/
```

```
msiecfexport -m all './Johnatan/Local Settings/History/History.IE5/index.dat'|tee ~/Escritorio/pf
#+END_SRC
```

Del análisis de este fichero [[./johnatan_IE5_index_dat.txt]] podemos obtener información de la navegación del usuario, ficheros descargados, etc

```
#+BEGIN_EXAMPLE
Record type : URL
Offset range : 23808 - 24192 (384)
Location : Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=Inbox&reset=1&YY=9873
Primary time : Feb 05, 2006 20:43:11.328000000
Secondary time : Feb 05, 2006 20:43:11.328000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 20:43:12
Cache directory index : -2 (0xfe)

Record type : URL
Offset range : 24192 - 24448 (256)
Location : Visited: Johnatan@http://70.107.249.150:8080/clientes.wmf
Primary time : Feb 05, 2006 20:44:10.156000000
Secondary time : Feb 05, 2006 20:44:10.156000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 20:44:12
Cache directory index : -2 (0xfe)

Record type : URL
Offset range : 24576 - 24960 (384)
Location : Visited: Johnatan@http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJ0KMsfYBZnaFKx
Primary time : Feb 05, 2006 20:44:11.281000000
Secondary time : Feb 05, 2006 20:44:11.281000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 20:44:12
Cache directory index : -2 (0xfe)

Record type : URL
Offset range : 24960 - 25344 (384)
Location : Visited: Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowFolder?rb=Inbox&reset=1&YY=2643
Primary time : Feb 05, 2006 20:43:16.546000000
Secondary time : Feb 05, 2006 20:43:16.546000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 20:43:18
Cache directory index : -2 (0xfe)
#+END_EXAMPLE
```

** Análisis de tiempos de acceso a URLs (Johnatan)

Datos de acceso de ~Johnatan~ al ERP para el timeline.

```
#+NAME:j_typedurls_tln
```

```
#+BEGIN_SRC src
# Obtenemos los documentos recientemente accedidos
cd /media/investigador/Documents and Settings/Johnatan
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p typedurls_tln
#+END_SRC

#+BEGIN_EXAMPLE
Launching typedurls v.20120827
1139178008|REG|||TypedURLs - url1: http://127.0.0.1/web-erp
#+END_EXAMPLE

** Documentos recientes (ver0k)

Los documentos recientes accedidos por ~ver0k~, y se observa que en muy
poco tiempo tiene una gran actividad.

#+NAME:v_recentdocs
#+BEGIN_SRC src
# Obtenemos los documentos recientemente accedidos
cd /media/investigador/Documents and Settings/ver0k
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p recentdocs
#+END_SRC

#+BEGIN_EXAMPLE
Launching recentdocs v.20100405
recentdocs v.20100405
(NTUSER.DAT) Gets contents of user's RecentDocs key

RecentDocs
**All values printed in MRUList\MRUListEx order.
Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
LastWrite Time Sun Feb  5 21:58:56 2006 (UTC)
  18 = Administrator's Documents
  37 = examen.gif
  36 = Apache
  35 = ABOUT_APACHE.TXT
  34 = maick
  33 = Sti_Trace.log
  32 = RRGEPPortadas.doc
  31 = RRGEPNotas.doc
  30 = Notas.doc
  24 = Indice Pormenorizado.doc
  29 = ÍNDICE DOCTORADO.doc
  28 = formulario.doc
  23 = 30SEP_bolecart-book.doc
  26 = Israel Robledo Gonzáles's Documents
  27 = concha.doc
  25 = Boletin11.doc
  19 = modelos
```

```
  22 = nm06082003.jpeg
  21 = nm06052003.jpeg
  20 = nm06042003.jpeg
  10 = nm06032003.jpeg
  9 = a017.jpg
  7 = imagenes
  8 = overlay_por_2006020110007_20060201224249.jpg
  6 = overlay_por_2006020107034_20060201190204.jpg
  17 = overlay_9_2006020110006.jpg
  16 = overlay_8_2006020110005.jpg
  15 = overlay_8.jpg
  14 = overlay_7_2006020110005.jpg
  13 = overlay_6_2006020110004.jpg
  12 = overlay_6_2005112211035.jpg
  11 = overlay_5_2006020110004.jpg
  4 = Local Disk (C:)
  5 = users.txt
  3 = clientes.txt
  1 = web-erp
  2 = config.php
  0 = AccountGroups.php

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc
LastWrite Time Sun Feb  5 21:47:42 2006 (UTC)
MRUListEx = 8,7,1,6,5,4,0,3,2
  8 = RRGEPPortadas.doc
  7 = RRGEPNotas.doc
  1 = Notas.doc
  6 = Indice Pormenorizado.doc
  5 = ÍNDICE DOCTORADO.doc
  4 = formulario.doc
  0 = 30SEP_bolecart-book.doc
  3 = concha.doc
  2 = Boletin11.doc

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gif
LastWrite Time Sun Feb  5 21:58:55 2006 (UTC)
MRUListEx = 0
  0 = examen.gif

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpeg
LastWrite Time Sun Feb  5 21:19:05 2006 (UTC)
MRUListEx = 3,2,1,0
  3 = nm06082003.jpeg
  2 = nm06052003.jpeg
  1 = nm06042003.jpeg
  0 = nm06032003.jpeg

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
```

```
LastWrite Time Sun Feb  5 21:18:05 2006 (UTC)
MRUListEx = 4,3,2,1,0,9,8,7,6,5
  4 = a017.jpg
  3 = overlay_por_2006020110007_20060201224249.jpg
  2 = overlay_por_2006020107034_20060201190204.jpg
  1 = overlay_9_2006020110006.jpg
  0 = overlay_8_2006020110005.jpg
  9 = overlay_8.jpg
  8 = overlay_7_2006020110005.jpg
  7 = overlay_6_2006020110004.jpg
  6 = overlay_6_2005112211035.jpg
  5 = overlay_5_2006020110004.jpg

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log
LastWrite Time Sun Feb  5 21:49:52 2006 (UTC)
MRUListEx = 0
  0 = Sti_Trace.log

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.php
LastWrite Time Sun Feb  5 20:50:02 2006 (UTC)
MRUListEx = 1,0
  1 = config.php
  0 = AccountGroups.php

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
LastWrite Time Sun Feb  5 21:53:46 2006 (UTC)
MRUListEx = 2,1,0
  2 = ABOUT_APACHE.TXT
  1 = users.txt
  0 = clientes.txt

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
LastWrite Time Sun Feb  5 21:58:56 2006 (UTC)
MRUListEx = 8,7,2,6,5,3,1,0
  8 = Administrator's Documents
  7 = Apache
  2 = maick
  6 = Israel Robledo Gonzáles's Documents
  5 = modelos
  3 = imagenes
  1 = Local Disk (C:)
  0 = web-erp
#+END_EXAMPLE

** Urls accedidas (ver0k)

Vemos que ~ver0k~ no ha accedido al navegador, ya que la URL es la
dirección de la web de ~MSN~.
```

```
#+NAME:v_typedurls
#+BEGIN_SRC src
# Obtenemos las URLs accedidas
cd /media/investigador/Documents and Settings/ver0k
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p typedurls
#+END_SRC

#+BEGIN_EXAMPLE
Launching typedurls v.20080324
typedurls v.20080324
(NTUSER.DAT) Returns contents of user's TypedURLs key.

TypedURLs
Software\Microsoft\Internet Explorer\TypedURLs
LastWrite Time Sun Feb  5 20:47:38 2006 (UTC)
  url1 -> http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=msnhome
#+END_EXAMPLE
```

Adicionalmente de ha extraido la información del fichero index.dat de su navegación y se ha guardado como evidencia.

```
#+NAME:v_IE5_index_dat
#+BEGIN_SRC src
# Obtenemos la información de index.dat
cd /media/investigador/Documents and Settings/
msiecfexport -m all './ver0k/Local Settings/History/History.IE5/index.dat'|tee ~/Escritorio/pfc/P
#+END_SRC
```

Del análisis de este fichero [[./ver0k_IE5_index_dat.txt]] podemos obtener información de la navegación del usuario, ficheros descargados y accedidos.

```
#+BEGIN_EXAMPLE
Record type : URL
Offset range : 21248 - 21504 (256)
Location : Visited: ver0k@file:///C:/users.txt
Primary time : Feb 05, 2006 21:06:37.562000000
Secondary time : Feb 05, 2006 21:06:37.562000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 21:06:38
Cache directory index : -2 (0xfe)

Record type : URL
Offset range : 21504 - 21888 (384)
Location : Visited: ver0k@http://messenger.msn.com/redirs/FIRST_TIME_EX.asp?GeoID=000000a6&Plcid=
Primary time : Feb 05, 2006 21:04:20.187000000
Secondary time : Feb 05, 2006 21:04:20.187000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 21:04:22
Cache directory index : -2 (0xfe)
```

```
Record type : URL
Offset range : 22144 - 22400 (256)
Location : Visited: ver0k@file:///C:/clientes.txt
Primary time : Feb 05, 2006 21:05:56.859000000
Secondary time : Feb 05, 2006 21:05:56.859000000
Expiration time : (0x0000 0x0000)
Last checked time : Feb 05, 2006 21:05:58
Cache directory index : -2 (0xfe)
#+END_EXAMPLE
```

** Análisis de tiempos de acceso a URLs (ver0k)

Datos de acceso de ~ver0k~ al ERP para el timeline.

```
#+NAME:v_typedurls_tln
#+BEGIN_SRC src
# Obtenemos los documentos recientemente accedidos
cd /media/investigador/Documents and Settings/ver0k
sudo perl /usr/share/regripper/rip.pl -r NTUSER.DAT -p typedurls_tln
#+END_SRC

#+BEGIN_EXAMPLE
Launching typedurls v.20120827
1139172458|REG|||TypedURLs - url1: http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar
#+END_EXAMPLE
```

** Analisis de la sesion de MSN Messenger (ver0k)

A raíz de identificar que el Administración instaló la herramienta MSN
se ha visto que el único usuario que lo utilizó es ~ver0k~.

Se analiza la información que encontramos una serie de ficheros
temporales bajo ~C:\Documents and Settings\ver0k\Application
Data\Microsoft\MSN Messenger\3817870080~, donde este ultimo numero es el
UserID generado a partir del nombre del usuario. [[http://www.msnfanatic.com/articles/how-to
se averigua que este userID se genera de la siguiente forma:

```
#+BEGIN_EXAMPLE
int getUserId(LPTSTR user)
 {
    unsigned int x = 0;
    for (int i = 0; i < strlen(user); i++) {
        x = x * 101;
        x = x + towlower(user[i]);
    }
return x;
 }
#+END_EXAMPLE
```

Aunque no es posible obtener el nombre de usuario a partir del UserID,
si es posible comprobar si una determinada direccion de correo genera
ese mismo UserID.

Dado que entre la información recabada por bulk-extractor hay una serie
de direcciones de correo obtenidas mediante el procedimiento de file
carving, se desarrolló un programa para generar el UserID de todos los
casos obteniendo un match: ~h4ckIII@hotmail.com~, lo que nos confirma
que fue esta la cuenta empleada por el atacante.

Adicionalmente se confirma ademas por el hecho de encontrar en el
fichero

~C:\Documents and Settings\ver0k\NTUSER.DAT~ la siguiente entrada:
~Software\Microsoft\CurrentVersion\UnreadMail\h4ckIII@hotmail.com~

Buscando la cadena ~h4ckIII~ en los resultados de bulk-extractor
y accediendo a posiciones de memoria concretas de la imagen se obtiene
información referente a otra dirección ~h4ckiii-2@hotmail.com~.

#+BEGIN_EXAMPLE
INVITE MSNMSGR:h4ckiii-2@hotmail.com MSNSLP/1.0
To: <msnmsgr:h4ckiii-2@hotmail.com>
#+END_EXAMPLE

Se sospecha que esta es la vía por la que se ha podido sacar información
si bien no se tienen evidencias de tal actividad.

** Identificación de virus y malware

Se ejecuta [[http://www.clamav.net/index.html][ClamAV]] y se identifica el fichero ~explorer.exe~
directorio ~My Documents~ del usuario ~Administrator~ infectado por
~Win.Trojan.Clons-725~.

La salida completa de la ejecución del antivirus se puede consultar en
[[./clamav.org]]

#+BEGIN_EXAMPLE
....
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/examen.gif
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/explorer.exe
/media/investigador/Documents and Settings/Administrator/My Documents/explorer.exe: Win.Trojan.Cl
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/Firefox Setup 1.5.
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/fondo.jpg
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/formulario.doc
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/GNOME-MagnesiumPun
Scanning /media/investigador/Documents and Settings/Administrator/My Documents/imagen.jpg
....

```
----------- SCAN SUMMARY -----------
Known viruses: 3846131
Engine version: 0.98.7
Scanned directories: 1710
Scanned files: 17609
Infected files: 1
Data scanned: 2340.11 MB
Data read: 2561.58 MB (ratio 0.91:1)
Time: 348.284 sec (5 m 48 s)
#+END_EXAMPLE
```

** Otros ficheros identificados

Software de seguridad para el uso del ~Administrator~ en ~\Documents & Settings\Administrator\My Documents\Sof7w4r3~:

- [[http://www.nirsoft.net/utils/cports.html][CurrPorts v.1.07]], una utilidad para listar l
  abiertos en el sistema.

- TCPView 2.40, una utilidad de www.sysinternals.com con el mismo
  proposito que la anterior.

- GFI LANguard Network Security Scanner v6.0 [18], que aunque presente
  no llego a instalarse en el sistema.

** Análisis de los resultados de bulk-extractor

Se observa que en distintos ficheros ~url.txt~, ~domain.txt~ , ~rfc822~ hay muchas entradas entorno a la posición de memoria 0x38F83CFA.

Se analiza:

```
#+BEGIN_EXAMPLE
38F83164   6A 6E 4A 65  70 2E 36 38  74 7A 32 67  5A 54 49 43  43 46 6B 72  4F 77 58 39  44
38F83188   71 41 5F 33  74 2E 46 35  74 44 61 6D  4E 71 71 6A  5A 4D 72 4E  33 58 4A 4D  62
38F831AC   32 69 75 50  58 31 59 45  4F 79 50 52  72 36 59 30  76 31 78 74  76 63 46 34  64
38F831D0   64 78 3D 30  26 53 65 61  72 63 68 3D  26 50 52 49  4E 54 3D 31  26 53 68 6F  77
38F831F4   38 35 39 30  37 26 6F 72  64 65 72 3D  64 6F 77 6E  26 73 6F 72  74 3D 64 61  74
38F83218   77 3D 61 26  68 65 61 64  3D 62 22 20  74 61 72 67  65 74 3D 5F  62 6C 61 6E  6B
38F8323C   F3 6E 20 69  6D 70 72 69  6D 69 62 6C  65 3C 2F 61  3E 0A 20 45  73 74 65 20  6D
38F83260   73 74 E1 20  6D 61 72 63  61 64 6F 20  63 6F 6E 20  75 6E 61 20  62 61 6E 64  65
38F83284   65 66 3D 22  2F 79 6D 2F  53 68 6F 77  4C 65 74 74  65 72 3F 62  6F 78 3D 25  34
38F832A8   73 67 49 64  3D 34 32 32  34 5F 30 5F  32 32 5F 31  31 34 38 5F  31 35 35 5F  30
38F832CC   59 6B 59 6E  34 55 72 36  52 67 39 57  75 4A 66 53  4D 5A 2E 53  30 2E 75 76  61
38F832F0   68 57 36 70  4C 71 32 69  32 33 41 77  4E 76 59 57  6A 36 79 54  71 4C 74 6A  6E
38F83314   54 49 43 43  46 6B 72 4F  77 58 39 44  2E 35 5F 69  6C 7A 45 58  36 45 63 71  41
38F83338   71 71 6A 5A  4D 72 4E 33  58 4A 4D 62  5F 69 62 70  6F 35 37 2E  46 6D 39 32  69
38F8335C   36 59 30 76  31 78 74 76  63 46 34 64  4D 69 37 42  78 49 41 63  2D 26 49 64  78
38F83380   46 4C 47 3D  31 26 59 59  3D 38 35 39  30 37 26 6F  72 64 65 72  3D 64 6F 77  6E
```

```
38F833A4   70 6F 73 3D  30 26 76 69  65 77 3D 61  26 68 65 61  64 3D 62 22  3E 4D 61 72  63 61 72
38F833C8   2F 61 3E 20  2D 20 3C 61  20 68 72 65  66 3D 22 2F  79 6D 2F 53  68 6F 77 4C  65 74 74
38F833EC   30 42 25 34  30 42 75 6C  6B 26 4D 73  67 49 64 3D  34 32 32 34  5F 30 5F 32  32 5F 31
38F83410   5F 32 5F 2D  31 5F 30 5F  6F 53 4F 59  6B 59 6E 34  55 72 36 52  67 39 57 75  4A 66 53
38F83434   79 58 52 66  47 72 4D 32  75 55 72 68  57 36 70 4C  71 32 69 32  33 41 77 4E  76 59 57
38F83458   4A 65 70 2E  36 38 74 7A  32 67 5A 54  49 43 43 46  6B 72 4F 77  58 39 44 2E  35 5F 69
38F8347C   5F 33 74 2E  46 35 74 44  61 6D 4E 71  71 6A 5A 4D  72 4E 33 58  4A 4D 62 5F  69 62 70
38F834A0   75 50 58 31  59 45 4F 79  50 52 72 36  59 30 76 31  78 74 76 63  46 34 64 4D  69 37 42
38F834C4   3D 30 26 53  65 61 72 63  68 3D 26 55  4E 52 3D 31  26 2E 63 72  75 6D 62 3D  5A 39 54
38F834E8   59 59 3D 38  35 39 30 37  26 6F 72 64  65 72 3D 64  6F 77 6E 26  73 6F 72 74  3D 64 61
38F8350C   76 69 65 77  3D 61 26 68  65 61 64 3D  62 22 3E 4D  61 72 63 61  72 20 63 6F  6D 6F 20
38F83530   2F 61 3E 20  5D 0A 09 09  09 09 09 09  3C 2F 70 3E  0A 3C 2F 64  69 76 3E 0A  3C 21 2D
38F83554   4F 43 20 2D  2D 3E 09 09  09 09 09 0A  09 09 09 09  09 0A 09 3C  21 2D 2D 20  74 79 70
38F83578   6E 6F 77 6E  20 2D 2D 3E  0A 0A 09 09  09 09 09 09  09 09 09 3C  74 61 62 6C  65 20 63
38F8359C   61 67 65 68  65 61 64 65  72 20 63 65  6C 6C 73 70  61 63 69 6E  67 3D 30 20  63 65 6C
38F835C0   30 20 77 69  64 74 68 3D  22 31 30 30  25 22 20 62  6F 72 64 65  72 3D 30 3E  0A 3C 74
38F835E4   73 73 3D 6C  61 62 65 6C  20 6E 6F 77  72 61 70 3E  44 65 3A 3C  2F 74 64 3E  3C 74 64
38F83608   79 63 73 61  2E 63 6F 6D  2E 6D 78 26  6E 62 73 70  3B 26 6E 62  73 70 3B 3C  61 20 68
38F8362C   73 63 72 69  70 74 3A 64  6F 63 75 6D  65 6E 74 2E  66 72 6D 41  64 64 41 64  64 72 73
38F83650   22 3E 3C 69  6D 67 20 73  72 63 3D 22  68 74 74 70  3A 2F 2F 75  73 2E 69 31  2E 79 69
38F83674   2E 79 69 6D  67 2E 63 6F  6D 2F 69 2F  75 73 2F 70  69 6D 2F 65  6C 2F 61 62  6F 6F 6B
38F83698   66 22 20 61  6C 69 67 6E  3D 74 6F 70  20 76 73 70  61 63 65 3D  30 20 68 73  70 61 63
38F836BC   72 3D 30 20  61 6C 74 3D  22 41 F1 61  64 69 72 20  61 20 4C 69  62 72 65 74  61 20 64
38F836E0   6F 73 22 20  77 69 64 74  68 3D 31 36  20 68 65 69  67 68 74 3D  31 36 3E 41  F1 61 64
38F83704   65 74 61 20  64 65 20 63  6F 6E 74 61  63 74 6F 73  3C 2F 61 3E  3C 2F 74 64  3E 3C 2F
38F83728   74 64 20 63  6C 61 73 73  3D 6C 61 62  65 6C 20 6E  6F 77 72 61  70 3E 50 61  72 61 3A
38F8374C   6A 6F 6E 61  74 68 61 6E  2E 74 65 7A  63 61 40 79  61 68 6F 6F  2E 63 6F 6D  3C 2F 74
38F83770   74 72 3E 3C  74 64 20 63  6C 61 73 73  3D 6C 61 62  65 6C 20 6E  6F 77 72 61  70 3E 41
38F83794   64 3E 3C 74  64 3E 20 55  72 67 65 6E  74 65 21 21  3C 2F 74 64  3E 3C 2F 74  72 3E 0A
38F837B8   6C 61 73 73  3D 6C 61 62  65 6C 20 6E  6F 77 72 61  70 3E 46 65  63 68 61 3A  3C 2F 74
38F837DC   6E 2C 20 20  35 20 46 65  62 20 32 30  30 36 20 31  34 3A 31 31  3A 31 33 20  2D 30 36
38F83800   2F 74 64 3E  3C 2F 74 72  3E 0A 3C 2F  74 61 62 6C  65 3E 0A 3C  66 6F 72 6D  20 6E 61
38F83824   41 64 64 72  73 20 61 63  74 69 6F 6E  3D 22 68 74  74 70 3A 2F  2F 61 64 64  72 65 73
38F83848   68 6F 6F 2E  63 6F 6D 2F  79 61 62 2F  65 31 3F 76  3D 59 4D 26  2E 72 61 6E  64 3D 32
38F8386C   73 69 6D 70  3D 31 22 20  6D 65 74 68  6F 64 3D 22  70 6F 73 74  22 3E 0A 3C  69 6E 70
38F83890   68 69 64 64  65 6E 22 20  6E 61 6D 65  3D 22 66 6E  22 20 76 61  6C 75 65 3D  22 22 3E
38F838B4   79 70 65 3D  22 68 69 64  64 65 6E 22  20 6E 61 6D  65 3D 22 6C  6E 22 20 76  61 6C 75
38F838D8   70 75 74 20  74 79 70 65  3D 22 68 69  64 64 65 6E  22 20 6E 61  6D 65 3D 22  65 22 20
38F838FC   6F 70 65 7A  40 65 79 63  73 61 2E 63  6F 6D 2E 6D  78 22 3E 0A  3C 69 6E 70  75 74 20
38F83920   64 65 6E 22  20 6E 61 6D  65 3D 22 2E  64 6F 6E 65  22 20 76 61  6C 75 65 3D  22 68 74
38F83944   33 37 36 2E  6D 61 69 6C  2E 79 61 68  6F 6F 2E 63  6F 6D 2F 79  6D 2F 62 6C  6F 63 6B
38F83968   73 67 49 64  3D 34 32 32  34 5F 30 5F  32 32 5F 31  31 34 38 5F  31 35 35 5F  30 5F 32
38F8398C   59 6B 59 6E  34 55 72 36  52 67 39 57  75 4A 66 53  4D 5A 2E 53  30 2E 75 76  61 79 58
38F839B0   68 57 36 70  4C 71 32 69  32 33 41 77  4E 76 59 57  6A 36 79 54  71 4C 74 6A  6E 4A 65
38F839D4   54 49 43 43  46 6B 72 4F  77 58 39 44  2E 35 5F 69  6C 7A 45 58  36 45 63 71  41 5F 33
38F839F8   71 71 6A 5A  4D 72 4E 33  58 4A 4D 62  5F 69 62 70  6F 35 37 2E  46 6D 39 32  69 75 50
38F83A1C   36 59 30 76  31 78 74 76  63 46 34 64  4D 69 37 42  78 49 41 63  2D 26 6F 72  64 65 72
38F83A40   3D 26 73 6F  72 74 3D 64  61 74 65 26  76 69 65 77  3D 61 26 68  65 61 64 3D  62 26 62
38F83A64   6B 26 59 59  3D 38 35 39  30 37 26 2E  63 72 75 6D  62 3D 59 33  2E 41 50 43  30 74 48
```

```
38F83A88   70 65 7A 40  65 79 63 73  61 2E 63 6F  6D 2E 6D 78  26 49 53 4E  53 50 41 4D  3D
38F83AAC   3C 69 6E 70  75 74 20 74  79 70 65 3D  22 68 69 64  64 65 6E 22  20 6E 61 6D  65
38F83AD0   6C 75 65 3D  22 68 74 74  70 3A 2F 2F  65 31 2E 66  33 37 36 2E  6D 61 69 6C  2E
38F83AF4   6D 2F 53 68  6F 77 4C 65  74 74 65 72  3F 4D 73 67  49 64 3D 34  32 32 34 5F  30
38F83B18   35 5F 30 5F  32 5F 2D 31  5F 30 5F 6F  53 4F 59 6B  59 6E 34 55  72 36 52 67  39
38F83B3C   75 76 61 79  58 52 66 47  72 4D 32 75  55 72 68 57  36 70 4C 71  32 69 32 33  41
38F83B60   74 6A 6E 4A  65 70 2E 36  38 74 7A 32  67 5A 54 49  43 43 46 6B  72 4F 77 58  39
38F83B84   63 71 41 5F  33 74 2E 46  35 74 44 61  6D 4E 71 71  6A 5A 4D 72  4E 33 58 4A  4D
38F83BA8   39 32 69 75  50 58 31 59  45 4F 79 50  52 72 36 59  30 76 31 78  74 76 63 46  34
38F83BCC   6F 72 64 65  72 3D 64 6F  77 6E 26 69  6E 63 3D 26  73 6F 72 74  3D 64 61 74  65
38F83BF0   64 3D 62 26  62 6F 78 3D  40 42 40 42  75 6C 6B 26  59 59 3D 38  35 39 30 37  22
38F83C14   09 09 09 09  09 09 0A 09  09 20 20 20  20 20 20 20  20 20 20 20  20 20 20 20  20
38F83C38   20 69 64 3D  6D 65 73 73  61 67 65 3E  0A 0A 09 09  09 09 3C 21  2D 2D 20 74  79
38F83C5C   2D 3E 0A 0A  3C 70 72 65  3E 3C 74 74  3E 4A 6F 68  6E 6E 79 3A  0A 0A 50 6F  72
38F83C80   20 65 6C 20  63 61 74 61  6C 6F 67 6F  20 71 75 65  20 65 73 74  61 20 65 6E  0A
38F83CA4   74 74 70 3A  2F 2F 37 30  2E 31 30 37  2E 32 34 39  2E 31 35 30  2F 63 6C 69  65
38F83CC8   61 72 67 65  74 3D 5F 62  6C 61 6E 6B  20 20 6F 6E  63 6C 69 63  6B 3D 22 72  65
38F83CEC   6E 6B 57 61  72 6E 69 6E  67 28 29 22  20 3E 68 74  74 70 3A 2F  2F 37 30 2E  31
38F83D10   63 6C 69 65  6E 74 65 73  2E 77 6D 66  3C 2F 61 3E  0A 0A 41 6C  62 65 72 74  6F
38F83D34   63 74 6F 72  20 47 65 6E  65 72 61 6C  0A 45 6C 65  63 74 72 6F  6E 69 63 61  20
38F83D58   6F 6E 20 53  2E 41 2E 20  64 65 20 43  2E 56 2E 0A  3C 2F 74 74  3E 3C 2F 70  72
38F83D7C   20 3C 21 2D  2D 20 74 6F  63 74 79 70  65 20 3D 20  58 2D 75 6E  6B 6E 6F 77  6E
38F83DA0   09 09 20 20  09 09 20 20  3C 21 2D 2D  20 74 6F 63  74 79 70 65  20 3D 20 74  65
38F83DC4   20 20 3C 21  2D 2D 20 74  65 78 74 20  2D 2D 3E 0A  09 09 20 20  20 20 09 09  20
38F83DE8   0A 0A 3C 2F  64 69 76 3E  0A 0A 0A 0A  09 09 09 09  09 3C 21 2D  2D 20 45 4E  44
38F83E0C   09 0A 0A 09  09 09 09 09  3C 66 6F 72  6D 20 6E 61  6D 65 3D 73  68 6F 77 4C  65
38F83E30   64 3D 70 6F  73 74 20 61  63 74 69 6F  6E 3D 22 2F  79 6D 2F 53  68 6F 77 4C  65
38F83E54   53 65 61 72  63 68 3D 26  59 59 3D 38  35 39 30 37  26 6F 72 64  65 72 3D 64  6F
38F83E78   65 26 70 6F  73 3D 30 26  76 69 65 77  3D 61 26 68  65 61 64 3D  62 22 3E 0A  3C
38F83E9C   68 69 64 64  65 6E 20 6E  61 6D 65 3D  22 2E 63 72  75 6D 62 22  20 76 61 6C  75
38F83EC0   43 73 59 22  3E 09 09 09  09 09 09 3C  69 6E 70 75  74 20 74 79  70 65 3D 68  69
38F83EE4   4D 73 67 49  64 22 20 76  61 6C 75 65  3D 22 34 32  32 34 5F 30  5F 32 32 5F  31
38F83F08   5F 2D 31 5F  30 5F 6F 53  4F 59 6B 59  6E 34 55 72  36 52 67 39  57 75 4A 66  53
38F83F2C   52 66 47 72  4D 32 75 55  72 68 57 36  70 4C 71 32  69 32 33 41  77 4E 76 59  57
38F83F50   70 2E 36 38  74 7A 32 67  5A 54 49 43  43 46 6B 72  4F 77 58 39  44 2E 35 5F  69
38F83F74   74 2E 46 35  74 44 61 6D  4E 71 71 6A  5A 4D 72 4E  33 58 4A 4D  62 5F 69 62  70
38F83F98   58 31 59 45  4F 79 50 52  72 36 59 30  76 31 78 74  76 63 46 34  64 4D 69 37  42
38F83FBC   70 75 74 20  74 79 70 65  3D 68 69 64  64 65 6E 20  6E 61 6D 65  3D 22 62 6F  78
38F83FE0   40 42 75 6C  6B 22 3E 0A  3C 69 6E 70  75 74 20 74  79 70 65 3D  68 69 64 64  65
#+END_EXAMPLE
```

Se obtiene el siguiente mensaje:

```
#+BEGIN_EXAMPLE
De: alopez@eycsa.com.mx
Para: jonathan.tezca@yahoo.com
Asunto: Urgente!!
Fecha: Sun, 5 Feb 2006 14:11:13 -0600 (CST)
Johnny:
```

Por favor baja el catalogo que esta en http://70.107.249.150/clientes.wmf
Alberto Lopez
Director General
Electronica y Computacion S.A. de C.V.
#+END_EXAMPLE

** Líneas de tiempo de los ficheros de la imagen

He intentado utilizar [[http://www.sleuthkit.org/sleuthkit/man/mmls.html][mmls]] y [[http://www.s
fichero de imagen facilitado no se ha podido utilizar.

He utilizado [[http://www.sleuthkit.org/mac-robber/index.php][mac-robber]] para recoger toda la i
ficheros del sistema analizado:

#+NAME:mac_robber
#+BEGIN_SRC sh
cd /media/investigador
mac-robber ./|tee ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/poc_mac_robber.mac
#+END_SRC

Se puede ver las salida en el fichero [[./poc_mac_robber.mac]].

A continuación se utiliza [[http://wiki.sleuthkit.org/index.php?title%3DMactime][mactime]] para d
al contenido obtenido en el paso anterior:

#+NAME:mactime
#+BEGIN_SRC sh
mactime -b ~/Escritorio/pfc/PoC-PFC-001/3_EVIDENCIAS/poc_mac_robber.mac -z EST5EDT |tee ~/Escrito
#+END_SRC

Y se puede ver el resultado en el fichero [[./poc_mactime.txt]].
** Análisis de eventos de windows

Event logs, en sus tres grupos de System, Security y Applications. En
concreto, el log de Security proporciona una gran cantidad de
informacion, por cuanto el sistema de auditoria de Windows esta
configurado para registrar la maxima cantidad de informacion, como por
ejemplo la creacion y fin de cualquier proceso en el sistema, el logon y
logout de un usuario, etc

** Apache Web Server

Los logs del servidor web Apache, tanto de acceso como de error, bajo
~C:\apache\Apache\logs~.

Se identifican distintos tipos de peticiones, algunos no correctamente
formados como:

#+BEGIN_EXAMPLE

```
[Sun Jan 29 17:01:43 2006] [error] [client 134.186.42.18] client sent
HTTP/1.1 request without hostname (see RFC2616 section 14.23):
/w00tw00t.at.ISC.SANS.DFind:)
#+END_EXAMPLE
```

y otros relacionados con la herramienta [[https://cirt.net/Nikto2][nikto]], utilizada para r
análisis de vulnerabilidades.

```
#+BEGIN_EXAMPLE
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does
not exist: c:/apache/apache/htdocs/nikto-1.35-d3ng4mwwxva0fqq8.htm
#+END_EXAMPLE
```

Esta herramienta es posteriormente utilizada contra el servidor web lo
que se puede ver en las siguientes líneas:

```
#+BEGIN_EXAMPLE
.........................................
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] attempt to invoke directory as s
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:30 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:31 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:31 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:31 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
[Mon Jan 30 17:28:31 2006] [error] [client 192.168.100.144] File does not exist: c:/apache/a
.........................................
#+END_EXAMPLE
```

** MySQL

Los logs de la base de datos MySQL, ~counters.log~ y ~counters.err~, bajo
~C:\apache\Apache\mysql\data\~.

```
** WebERP

[[http://www.weberp.org][WebERP v3.04]], instalado en el directorio
~C:\apache\Apache\htdocs\web-erp~, es un paquete open source para la
gestion de negocio (ERP).

Existen entradas de dos tipos:
- Arranque / parada.
- Autovacuum (limpieza) de la base de datos.
```

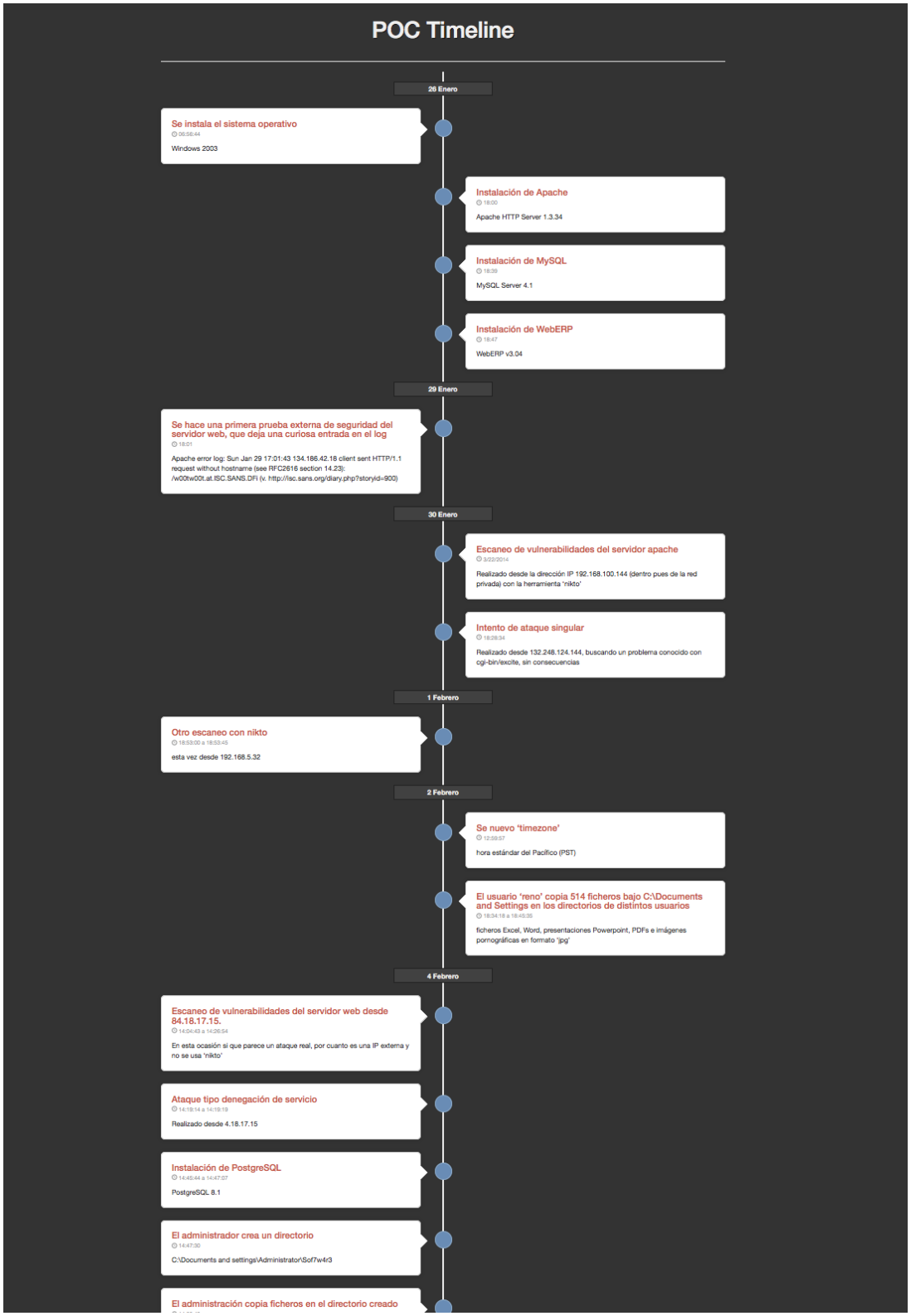
Línea temporal del suceso a investigar

La línea temporal del suceso a investigar es un gráfico que presenta, de una forma comprensible, los hitos más relevantes de la investigación.

Siguiendo con la filosofía del proyecto de utilizar Emacs para acometer todas las tareas, se ha optado por desarrollar la base de la línea temporal en Javascript.

Sin embargo la integración de la misma en el informe no es del todo satisfactoria, ya que el mismo está orientado a formato pdf. La alternativa sería utilizar un informe con formato accesible vía web, por temas estéticos y funcionales.

Tomando los datos del proceso de análisis se ha desarrollado una línea de tiempo vertical que está accesible en formato html, y que tiene el aspecto que se muestra a continuación:




```
<!doctype html>
<html lang='es-ES'>
<head>
  <meta charset='utf-8'>
  <meta http-equiv='Content-Type'' content='text/html'>
```

```
  <title>PoC Timeline</title>
  <meta name='author' content='José Luis Jerez'>
  <link rel='shortcut icon' href='http://static.tmimgcdn.com/img/favicon.ico'>
  <link rel='icon' href='http://static.tmimgcdn.com/img/favicon.ico'>
  <link rel='stylesheet' type='text/css' media='all' href='css/bootstrap.min.css'>
  <link rel='stylesheet' type='text/css' media='all' href='css/bootstrap-glyphicons.css'>
  <link rel='stylesheet' type='text/css' media='all' href='css/styles.css'>
  <script type='text/javascript' src='js/jquery-1.11.0.min.js'></script>
</head>

<body>
<div class='container'>
  <header class='page-header'>
    <h1>POC Timeline</h1>
  </header>

  <ul class='timeline'>
    <li><div class='tldate'>26 Enero</div></li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Se instala el sistema operativo</h4>
          <p><small class='text-muted'><i class='glyphicon
          glyphicon-time'></i> 06:56:44 </small></p>
        </div>
        <div class='tl-body'>
          <p>Windows 2003</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Instalación de Apache</h4>
          <p><small class='text-muted'>
          <i class='glyphicon glyphicon-time'>
          </i> 18:00</small></p>
        </div>
        <div class='tl-body'>
          <p>Apache HTTP Server 1.3.34</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
```

```
    <div class='tl-circ'></div>
    <div class='timeline-panel'>
      <div class='tl-heading'>
        <h4>Instalación de MySQL</h4>
        <p><small class='text-muted'>
        <i class='glyphicon glyphicon-time'>
        </i> 18:39</small></p>
      </div>
      <div class='tl-body'>
        <p>MySQL Server 4.1</p>
      </div>
    </div>
  </li>

  <li class='timeline-inverted'>
    <div class='tl-circ'></div>
    <div class='timeline-panel'>
      <div class='tl-heading'>
        <h4>Instalación de WebERP</h4>
        <p><small class='text-muted'>
        <i class='glyphicon glyphicon-time'>
        </i> 18:47</small></p>
      </div>
      <div class='tl-body'>
        <p>WebERP v3.04</p>
      </div>
    </div>
  </li>

  <li><div class='tldate'>29 Enero</div></li>

  <li>
    <div class='tl-circ'></div>
    <div class='timeline-panel'>
      <div class='tl-heading'>
        <h4>Se hace una primera prueba externa de seguridad del
servidor web, que deja una curiosa entrada en el log</h4>
        <p><small class='text-muted'>
        <i class='glyphicon glyphicon-time'>
        </i> 18:01</small></p>
      </div>
      <div class='tl-body'>
        <p>Apache error log: Sun Jan 29 17:01:43
           134.186.42.18 client sent
  HTTP/1.1 request without hostname (see RFC2616 section 14.23):
  /w00tw00t.at.ISC.SANS.DFi
  (v. http://isc.sans.org/diary.php?storyid=900)</p>
      </div>
    </div>
```

```
    </li>

    <li><div class='tldate'>30 Enero</div></li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Escaneo de vulnerabilidades del
servidor apache</h4>
          <p><small class='text-muted'>
          <i class='glyphicon glyphicon-time'>
          </i> 3/22/2014</small></p>
        </div>
        <div class='tl-body'>
          <p>Realizado desde la direccion IP
             192.168.100.144 (dentro pues de
la red privada) con la herramienta 'nikto'</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Intento de ataque singular</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 18:28:34</small></p>
        </div>
        <div class='tl-body'>
          <p>Realizado desde
132.248.124.144, buscando un problema
            conocido con cgi-bin/excite, sin
consecuencias</p>
        </div>
      </div>
    </li>

    <li><div class='tldate'>1 Febrero</div></li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4> Otro escaneo con nikto</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
```

```
  </i> 18:53:00 a 18:53:45</small></p>
        </div>
        <div class='tl-body'>
          <p>esta vez desde 192.168.5.32</p>
        </div>
      </div>
    </li>

    <li><div class='tldate'>2 Febrero</div></li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Se nuevo 'timezone' </h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:59:57</small></p>
        </div>
        <div class='tl-body'>
          <p>hora estandar del Pacifico (PST)</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>El usuario 'reno' copia 514 ficheros
bajo C:\Documents and Settings en los
            directorios de distintos
usuarios</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 18:34:18 a 18:45:35</small></p>
        </div>
        <div class='tl-body'>
          <p>ficheros Excel, Word, presentaciones Powerpoint,
PDFs e imagenes pornograficas en formato 'jpg'</p>
        </div>
      </div>
    </li>

    <li><div class='tldate'>4 Febrero</div></li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
```

```
        <div class='tl-heading'>
          <h4>Escaneo de vulnerabilidades del
servidor web desde 84.18.17.15.</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 14:04:43 a 14:26:54</small></p>
        </div>
        <div class='tl-body'>
          <p>En esta ocasion si que parece un
ataque real, por cuanto es una IP externa
y no se usa 'nikto'</p>
        </div>
      </div>
    </li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Ataque tipo denegacion de servicio</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 14:19:14 a 14:19:19</small></p>
        </div>
        <div class='tl-body'>
          <p>Realizado desde 4.18.17.15</p>
        </div>
      </div>
    </li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Instalacion de PostgreSQL</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 14:45:44 a 14:47:07</small></p>
        </div>
        <div class='tl-body'>
          <p>PostgreSQL 8.1</p>
        </div>
      </div>
    </li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
```

```
          <h4>El administrador crea un directorio</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 14:47:30</small></p>
        </div>
        <div class='tl-body'>
          <p>C:\Documents and settings\Administrator\Sof7w4r3</p>
        </div>
      </div>
    </li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>El administración copia ficheros en el
directorio creado</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 14:59:43</small></p>
        </div>
        <div class='tl-body'>
          <p>Tcpview.exe, languardnss6.exe y cports.exe.</p>
        </div>
      </div>
    </li>

    <li>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>El administrador crea otro
directorio</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 15:28:25</small></p>
        </div>
        <div class='tl-body'>
          <p>C:\Documents and Settings\Administrator\My Documents\update
que contiene algunos hotfixes a instalar</p>
        </div>
      </div>
    </li>

    <li><div class='tldate'>5 Febrero</div></li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
```

```
        <div class='tl-heading'>
          <h4>Comienzo del ataque</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:11:13</small></p>
        </div>
        <div class='tl-body'>
          <p>Alguien, en algún lugar,
crea un correo con el que intenta conseguir
que un usuario del sistema
(Johnatan) acceda a una URL determinada,
mediante la cual tiene
previsto conseguir acceso al sistema</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>El usuario Johnatan hace login en el sistema</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:23:09</small></p>
        </div>
        <div class='tl-body'>
          <p>Es
particularmente importante porque
es este usuario y en esta sesion el
que va a sufrir el ataque.</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Johnatan arranca el Internet Explorer</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:23:49</small></p>
        </div>
        <div class='tl-body'>
          <p>Process ID 3128</p>
        </div>
      </div>
    </li>
```

```
    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Johnatan se conecta a mail.yahoo.com</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:26:46</small></p>
        </div>
        <div class='tl-body'>
          <p>Para leer su correo</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Primer intento de ataque. Johnatan ha caido en la
trampa y accede a http://70.107.249.150/clientes.wmf
  </h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:41:30</small></p>
        </div>
        <div class='tl-body'>
          <p> Sin embargo, el exploit falla y
no hayconsecuencias aparentes.</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Johnatan abre otro correo</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:43:44</small></p>
        </div>
        <div class='tl-body'>
          <p></p>
        </div>
      </div>
    </li>
```

```
    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Internet explorer advierte
a Johnatan de que el
contenido ha sido bloqueado. </h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:43:50</small></p>
        </div>
        <div class='tl-body'>
          <p>Pero este ignora la advertencia y sigue
adelante.</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Se accede a http://70.107.249.150:8080/clientes.wmf</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:44:10</small></p>
        </div>
        <div class='tl-body'>
          <p>Es la misma dirección que el anterior
pero diferente puerto</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>¡¡¡EXPLOIT!!! El atacante arranca un interprete
de comandos en el sistema accesible desde el exterior</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:44:11</small></p>
        </div>
        <div class='tl-body'>
          <p>Ademas, como
Johnatan pertenece al grupo Administrators,
con privilegios de
Administrador.</p>
```

```
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>El atacante anade la cuenta ver0k</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:45:30</small></p>
        </div>
        <div class='tl-body'>
          <p>Con el comando 'net user
ver0k password /ADD'</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>Luego anade la cuenta ver0k al grupo
Administrators</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:45:53</small></p>
        </div>
        <div class='tl-body'>
          <p>Con el comando 'net group 'Administrators' ver0k /ADA'</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>el atacante cambia las entradas del registry que
permiten el acceso remoto al sistema </h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:46:23</small></p>
        </div>
        <div class='tl-body'>
          <p>En particular,
'HKLM\SYSTEM\CurrentControlSet\Terminal Server\fDenyTSConenctions =0'
```

```
con Terminal Remoto: "REG ADD
'HKLM\System\CurrentControlSet\Control\Terminal Server' /v
fDenyTSConnections /t REG_DWORD /d 0 /f</p>
        </div>
      </div>
    </li>

    <li class='timeline-inverted'>
      <div class='tl-circ'></div>
      <div class='timeline-panel'>
        <div class='tl-heading'>
          <h4>El atacante ('ver0k') se conecta por
Terminal Remoto al sistema</h4>
          <p><small class='text-muted'>
  <i class='glyphicon glyphicon-time'>
  </i> 12:46:54 a 12:47:21</small></p>
        </div>
        <div class='tl-body'>
          <p>Desde la IP 70.107.249.155, distinta de la
anterior que era 70.107.249.150</p>
        </div>
      </div>
    </li>
  </ul>
</div>
</body>
</html>
```

Informe técnico

El informe técnico realizado, al igual que en los casos anteriores, se va a presentar a continuación en formato org, tal como se ha desarrollado.
Adicionalmente, para facilitar la lectura, se presenta en formato pdf (preferiblemente) y html.
El informe ha sido desarrollado siguiendo la metodología propuesta, al igual que el resto de tareas de la prueba de concepto, y en este caso particular, está preparado para importar datos de la plantilla de datos generales y que la generación del informe se realice (utilizando la función de emacs-lisp `gpgFilesToPdf` desarrollada para este proyecto) de forma segura.
Tal como se comenta en el análisis, el objetivo del proyecto es que el continente del mismo sea adecuado a la metodología, no siendo la calidad del contenido (en relación al alcance de la investigación y el detalle de su desarrollo forense) un objetivo principal, lo que no implica que la calidad del mismo sea baja.

```
,+EMAIL: jljerez at error0x01.net
,+DATE: 2015-06-19
,+TITLE: Informe técnico forense
,+AUTHOR: José Luis Jerez
,+OPTIONS: H:5 num:t TeX:t LaTeX:t skip:nil f:t |:t d:nil todo:nil pri:nil tags:nil toc:nil
,+STARTUP: overview hidestars lognotestate

#+STARTUP: align fold nodlcheck hidestars oddeven lognotestate overview
#+STARTUP: fninline fnadjust
```

```
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:{} _:{} -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+EXPORT_SELECT_TAGS: export
#+EXPORT_EXCLUDE_TAGS: noexport
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+INFOJS_OPT: view:showall toc:t ltoc:t mouse:underline path:http://orgmode.org/org-info.js
#+HTML_HEAD: <link rel='stylesheet' type='text/css' href='../../DOC_ANEXA/worg.css' />

#+LATEX_CLASS: article
#+LATEX_CLASS_OPTIONS: [a4paper]
#+EXPORT_EXCLUDE_TAGS: HIDDEN
#+LATEX_HEADER: \usepackage{gensymb}
#+LATEX_HEADER: \hypersetup{colorlinks=true,linkcolor=magenta}
#+LaTeX_HEADER: \usepackage[T1]{fontenc}
#+LaTeX_HEADER: \usepackage{libertine}
#+LaTeX_HEADER: \renewcommand*\oldstylenums[1]{{\fontfamily{fxlj}\selectfont #1}}
#+LaTeX_HEADER: \usepackage{lmodern}

#+LaTeX_HEADER: \usepackage{fancyhdr} % para que cuente paginas en blanco también
#+LaTeX_HEADER: \pagestyle{fancy}
#+LaTeX_HEADER: \usepackage[spanish,activeacute]{babel}
#+LaTeX_HEADER: \fancyhead[L]{19-06-2015}
#+LaTeX_HEADER: \usepackage{lastpage}
#+LaTeX_HEADER: \fancyhead[R]{PcC-ITF-001}
#+LaTeX_HEADER: \lfoot{Informe de investigación forense \\ III Reto forense UNAM 2014} % Tít
#+LaTeX_HEADER: \cfoot{}
#+LaTeX_HEADER: \rfoot{\thepage \ de \ \protect\pageref{LastPage}}
#+LaTeX_HEADER: \renewcommand{\headrulewidth}{0.4pt}
#+LaTeX_HEADER: \renewcommand{\footrulewidth}{0.4pt}

#+BIND: org-latex-title-command '\\titleGP'

#+LATEX_HEADER: \newcommand*{\titleGP}{\begingroup % Create the command for including the ti
#+LATEX_HEADER: \centering % Center all text
#+LATEX_HEADER: \vspace*{\baselineskip} % White space at the top of the page
#+LATEX_HEADER:
#+LATEX_HEADER: \rule{\textwidth}{1.6pt}\vspace*{-\baselineskip}\vspace*{2pt} % Thick horizo
#+LATEX_HEADER: \rule{\textwidth}{0.4pt}\\[\baselineskip] % Thin horizontal line
#+LATEX_HEADER:
#+LATEX_HEADER: {\LARGE Informe de investigación forense \\ - III Reto forense UNAM 2014 -}\
#+LATEX_HEADER:
#+LATEX_HEADER: \rule{\textwidth}{0.4pt}\vspace*{-\baselineskip}\vspace{3.2pt} % Thin horizo
#+LATEX_HEADER: \rule{\textwidth}{1.6pt}\\[\baselineskip] % Thick horizontal line
#+LATEX_HEADER:
#+LATEX_HEADER: \begin{flushleft}
#+LATEX_HEADER: \vfill
#+LATEX_HEADER: \vspace*{2\baselineskip}
```

```
#+LATEX_HEADER:
#+LATEX_HEADER: Cod. de expediente/procedimiento: EXP-000000\\[\baselineskip]
#+LATEX_HEADER: Técnico investigador: José Luis Jerez\\[\baselineskip]
#+LATEX_HEADER: Peticionario de la actuación: Francisco Monserrat (Red IRIS)\\[\baselineskip]
#+LATEX_HEADER: Destinatario del informe: Juez de la Sala primera de lo penal \\[\baselineskip]
#+LATEX_HEADER: Letrado: Fernando Pérez\\[\baselineskip]
#+LATEX_HEADER: Localización física del análisis: \href{https://www.google.es/maps/place/UPM+-+Ca
#+LATEX_HEADER: {\scshape Fecha de expedición: 19-06-2015} \\[0.3\baselineskip]
#+LATEX_HEADER: \end{flushleft}
#+LATEX_HEADER: \endgroup}
\vspace{3in}

\newpage
\tableofcontents
\newpage

* Declaración de tachas

En cumplimiento del artículo 343.1 de la [[http://www.boe.es/boe/dias/
2000/01/08/pdfs/A00575-00728.pdf][Ley 1/2000 del 7 de enero de
Enjuiciamiento Civil]], el técnico investigador manifiesta:

#+BEGIN_EXAMPLE
1. No ser conyuge o pariente por consanguinidad o afinidad, dentro del
cuarto grado civil de una de las partes o de sus abogados o
procuradores.

2. No tener interes directo o indirecto en el asunto o en otro semejante.

3. No estar o haber estado en situacion de dependencia o de comunidad o
contraposicion de intereses con alguna de las partes o con sus abogados
o procuradores.

4. No amistad intima o enemistad con cualquiera de las partes o sus
procuradores o abogados.

5. No cualquier otra circunstancia, debidamente acreditada, que les haga
desmerecer en el concepto profesional.
#+END_EXAMPLE

* Juramento o promesa

En cumplimiento del artículo 335.2 de la [[http://www.boe.es/boe/dias/
2000/01/08/pdfs/A00575-00728.pdf][Ley 1/2000 del 7 de enero de
Enjuiciamiento Civil]], prometo decir la verdad, y al emitir el presente
informe actúo con la mayor objetividad posible, tomando en consideracion
tanto lo que pueda favorecer como lo que sea susceptible de causar
perjuicio a cualquiera de las partes, y conozco las sanciones penales en
las que podria incurrir si incumpliere este deber como perito.
```

\newpage

* Índice general

El presente informe se compone de dos apartados iniciales:

- Declaración de tacha :: En este apartado se establece que el investigador puede aplicar el sistema de tachas o hacer constar su imparcialidad.
- Juramento o promesa :: En este apartao se establece que al emitir su dictamen, el investigador manifiesta bajo juramento o promesa de decir la verdad.

El cuerpo del informe se compone de los siguientes apartados:

+ *Objeto*. Aclara la finalidad del informe forense, e introducir qué es lo que se pretende con todo el trabajo realizado.

+ *Alcance*. Tal como indica su título, en este apartado se desarrolla el alcance de cada una de las cuestiones que se plantaron en el apartado anterior de forma que quede claro para el receptor del informe que se ha cumplido con los objetivos acordados, y, en caso de que el alcance se haya modificado durante el desarrollo del proyecto (siempre de mutuo acuerdo), que todo aparezca claramente reflejado. Además, se desarrollarán aspectos como los procesos, recursos, limitaciones, esfuerzo y presupuesto.

+ *Antecedentes*. Son los hechos acontecidos con anterioridad al inicio del análisis forense y que sirven de punto de partida del mismo.

  Sin embargo, los antecedentes no deben de condicionar el resultado del informe, y deben de tomarse como una fuente más de información que debe de ser tratada.

+ Consideraciones preliminares. Dado que el informe se desarrolla a posteriori, al redactar este apartado conocemos lo que pensábamos, como analistas previo a realizar el análisis y la certeza o errores de nuestras consideraciones previas. Aquí se desarrolla todo lo que el analista forense considere necesario para explicar las decisiones tomadas en función de la información que se tenía en ese momento, como se desarrolló el trabajo, qué bases teóricas dieron lugar a la utilización de una u otra tecnología, los procedimientos seguidos, así como las limitaciones y restricciones que existieron en cada momento.

  Toda esta información permitirá conocer y entender como se ha realizado el trabajo, porque se ha identificado y extraído

  determinadas evidencias y otras se han podido perder, y cómo se ha llegado a las conclusiones presentadas.

+ *Documentos de referencia*. Libros, documentos, manuales, normas, información obtenida de URLs, etc. Cualquier soporte, físico o electrónico, que haya sido utilizado para desarrollar el análisis forense.

+ Terminología y abreviaturas. Todos los términos tecnológicos y abreviaturas que se han usado en la redacción del informe.

+ *Proceso de análisis*

  + *Actuaciones*. (Equivale al proceso de análisis del informe del reto) Cada acción que ejecuta el analista forense debe de estar justificada previo a realizarla, y documentada durante todo el proceso, de modo que el analista forense se encuentre en disposición de contestar cualquier cuestión que se le plantee posteriormente.

Este apartado es especialmente importante el las actuaciones complejas, ya que la memoria no es fiable.

  + *Análisis*. (Equivale al análisis de atefactos). Toda la labor realizada por el analista debe de quedar, de la forma más explícita y resumida posible, plasmada y justificada en este apartado.

Debe de aparecer reflejado todo el proceso, fundamentado en buenas prácticas o experiencias previas a falta de las primeras, todas la situaciones que se han ido dando, la resolución de las mismas y cualquier explicación que permita comprender, sin lugar a dudas, el porque de cada paso dado y su necesidad.

Para toda aquella información que sea demasiado extensa o técnica se tendrá que evaluar la necesidad o idoneidad de que aparezca en este apartado o en los anexos, haciendo referencia a los mismos.

+ *Cronología de eventos*

+ *Línea temporal*

+ *Conclusiones*. (Incluye el alcance de la intrusión). Sólo deben de desarrollarse las conclusiones de las cuestiones planteadas. Ésas deben de ser:

  * Objetivas.

  * Precisas.

  * Claras.

  * Justificadas.

+ *RECOMENDACIONES*

  * En caso de que se soliciten como parte de la investigación digital. En un proceso forense no son necesarias ya que no forma parte del alcance.

+ *ANEJOS*.

  No existen normas predefinidas para este apartado. Cualquier aspecto que, por la razón que sea, no haya podido ser desarrollado a lo largo del informe se puede y debe de añadir en como anexo y deben de formar parte del mismo como cualquier otro punto, e incluirlos en el índice.

  * *Direcciones IP implicadas*

  * *Cualquier documento*, nota, fotografía que ayude a entender o reforzar el contenido de la pericial.

  * Temas técnicos tratados en profundidad.

  * Descripción de los *méritos*, menciones, titulaciones y certificaciones, experiencia y trayectoria que acreditan al *investigador forense* como experto en la materia sobre la que se ha realizado el informe.

  * Datos relativos a la fecha de solicitud del informe, el plazo dado para la realización del mismo y cualquier evento que haya podido modificar en el tiempo los resultados del análisis, como retrasos justificados o injustificados.

\newpage

* Cuerpo del informe
** Objeto

El acuerdo firmado presume la previa aceptación de la oferta asociada al proyecto con código {{{codProy}}} según los términos expresados en la misma.

Se autoriza a {{{nomProf}}} a realizar los trabajos de {{{tipoServ}}} sobre los activos identificados por {{{empCli}}}, permitiendo efectuar las pruebas correspondientes.

El activo analizado ha sido:

- {{{Activo_1}}}

Siguiendo la metodología IIFBE (Investigación Informática Forense Basada en Emacs) se han realizado las copias de seguridad necesarias para la preservación de las evidencias y las mismas han sido almacenadas siguiendo un procedimiento que permite asegurar la integridad y trazabilidad de las mismas.

Toda la investigación se ha realizado respetando la legislación vigente así como las políticas de {{{empCli}}}, y manteniendo las medidas de confidencialidad descritas en la metodología.

\newpage

** Alcance

Se ha cumplido con los objetivos acordados en el alcance de cada una de las cuestiones que se plantaron en el apartado anterior, sin modificar los objetivos del mismo.

En la siguiente tabla de acciones realizadas, obtenida del documento de [[../0_INF_BASE/PoC-RAR-001.org][registro de acciones realizadas]] presentado como parte de la documentación se puede ver la dedicación a las tareas de más alto nivel llevadas a cabo:

Headline	Time	
Total time	*5d 17:56*	
Proceso de Preparación	18:03	
\emsp Registro de acciones...		0:05
\emsp Plan de proyecto		13:38
\emsp Estructura de directorios		0:11
\emsp Acuerdo de confidencialidad		0:21
\emsp Antecedentes		0:32
\emsp Fichero de datos generales		0:23
\emsp Autorización y aceptación de trabajos		0:18
\emsp Registro de limitaciones y exclusiones		1:11
\emsp Documento de inicio de proyecto		1:24
Proceso de identificación	3:53	
\emsp Registro de incidencias		0:11
\emsp Identificación de palabras clave		0:13
\emsp Identificación de actores y cuadro...		1:50
\emsp Croquis del escenario		1:25
\emsp Identificación de activos involucrados		0:14
Proceso de recopilación (recolección...	0:55	
\emsp Cadena de custodia		0:55

Proceso de preservación	0:15	
\emsp Tiempo dedicado a la preservación de...		0:15
Proceso de análisis	3d 8:11	
\emsp Checklist de herramientas HW/SW		6:22
\emsp Checklist de artefactos		2:58
\emsp Análisis de datos y evidencias		2d 16:57
\emsp Cronología relacional o línea temporal		5:54
Proceso de consolidación	1d 10:39	
\emsp Informe técnico		1d 10:08
\emsp Documento de aceptación de fin de...		0:31

Adicionalmente, en el plan de proyecto ([[../1_PLANIFICACION/00-PFC-plan%3D2015-05-25%3D2015-06-25.html] [proyecto en html]] y [[../1_PLANIFICACION/40-jljerez-actual%3D2015-05-25%3D2015-06-25.html] [uso de recursos en html]])se presentan las tareas realizadas por el técnico investigador y en él se puede identificar el tiempo planificado para cada una de ellas y el invertido realmente.

[[./taskjuggler.png]]

Si bien los objetivos del proyecto no han sido modificados tal y como se ha comentado, si es cierto que el alcance se ha visto afectado por una serie de limitaciones que fueron notificadas al cliente y documentadas en su momento, y son:

#+tblname: POC-051114-001

Código	POC-051114-001
Exclusion/limite	Se excluye cualquier tipo de fuente de evidencias adicional a la imagen facilitada.
Motivo	Reglas del reto forense.
Responsable	Organización del reto.

#+tblname: POC-051114-002

Código	POC-051114-002
Exclusion/limite	Se excluyen entrevistas o información adicional por parte del cliente.
Motivo	Reglas del reto forense.

Responsable	Investigador.

#+tblname: POC-081114-001

Código	POC-081114-001
Exclusion/limite	Se excluye el acceso a datos personales localizados en la imagen facilitada.
Motivo	Contexto legal.
Responsable	Investigador.

\newpage

** Antecedentes

Como parte de la metodología utilizada para el desarrollo de la investigación, una de las primeras tareas realizadas ha sido la firma de un *[[../0_INF_BASE/PoC-AC-001.org.pdf][acuerdo de confidencialidad]]* con {{{empCli}}}, que se presenta como
parte de la documentación.

Se han tomado medidas de seguridad para la gestión de la información facilitada al técnico investigador con objeto de preservar la confidencialidad e integridad de la misma:

- Se ha trabajado en una *estructura de directorios desplegada sobre un sistema de ficheros cifrado.*
- Se ha trabajado con *ficheros cifrados* con un sistema de clave pública. Si bien se presentan descifrados como parte de la documentación de la investigación para facilitar su acceso, se dispone de una *copia cifrada y formada digitalmente* que será entregada como evidencia en caso de que ésta sea requerida.

Durante la investigación se ha desarrollado un *[[./0_INF_BASE/PoC_Datos_generales.org][fichero de datos generales]]* utilizado para la generación segura y consistente de algunos de los documentos presentados. Este método de trabajo asegura la consistencia de los datos ya que éstos siempre se obtienen del mismo origen.

Antecedentes iniciales

Los antecedentes iniciales obtenidos y documentados durante la preparación de la investigación son:

~Código de documento:~ [[../0_INF_BASE/PoC-ATC-001.org][PoC-ATC-001]]

~Lugar de reunion:~ {{{calleProf}}}

~Objetivo:~ Obtener la información referente a los antecedentes de la investigación.

~Responsable de la reunion:~ {{{nomCli}}}

~Fecha y Hora de inicio:~ [2015-05-29 Fri 15:01]

~Fecha y Hora de fin:~ [2015-05-29 Fri 18:22]

~Clasificación:~ CONFIDENCIAL

~Asuntos a tratar:~

- Sucesos identificados.
- Personal implicado.
- Sistemas implicados.

~ASISTENTES~

Nombre	Cargo
{{{nomCli}}}	{{{cargoCli}}}
{{{nomProf}}}	{{{tipoProf}}}

~Observaciones:~

En el caso que nos ocupa, no hay información adicional ni oportunidad de obtenerla.

La información relativa a los antecedentes se obtiene a
partir del enlace http://www.seguridad.unam.mx/eventos/reto/.

~Proxima reunion:~ No establecida

~ANTECEDENTES~

Num	Descripcion
	El administrador de sistemas de una pequeña empresa
	ha notado que existe una cuenta que él no creó en su

1	sistema de ERP (Enterprise Resource Planning), por lo que el administrador de sistemas sospecha de algún ingreso no autorizado, del que desconoce el alcance.
2	El sistema en que se ejecuta la aplicación es un servidor Windows 2003, cuya principal función era proporcionar acceso al sistema ERP aa través de la Web.
3	Hace poco tiempo que habían migrado al uso de este servidor.
4	Según el administrador, trataba de mantener el sistema actualizado por lo que no sabe cómo pudieron ingresar a su sistema.
5	El administrador mencionó que más de una persona tiene acceso a cuentas privilegiadas en el sistema y que a veces utilizan estas cuentas para labores administrativas y personales.
6	El administrador mencionó que los usuarios del servidor utilizan aplicaciones que no requieren ningún tipo de privilegio para ejecutarse.
7	Datos de la imagen del equipo comprometido: - Sistema Operativo de equipo comprometido: Windows 2003 - Tamaño de la imagen: <= 6 GB. - La firmas md5 de la imagen completa, comprimida y descomprimida, respectivamente, son: + 062cf5d1ccd000e20cf4c006f2f6cce4 - windows2003.img + 33a42d316c060c185f41bfcacf439747 - windows2003.img.gz

~COMENTARIOS DEL INVESTIGADOR~

Num	Descripcion
1	No se especifica ningún dato adicional acerca del ERP.
2	No se especifica ningún dato adicional acerca del servdor, como el nivel de parcheo o funcionalidades/aplicaciones adicionales del servidor que podrían ser relevantes para la investigación.
3	No se facilitan fechas, concretas ni aproximadas, relativas a la instalación o posible intrusión.

4	No se facilita información concreta acerca del nivel de parches instalados en el sistema o aplicativos instalados.	
5	No se facilita un listado de usuarios con acceso al sistema (ni por lo tanto sus contraseñas).	

~COMPROMISOS/ACUERDOS~

Num	Descripcion	Responsable	Fecha
1	firmar el documento de aceptación y autorización de trabajos	{{{nomProf}}}	
2			
3			

Una vez obtenida la información para la preparación del proyecto, como último paso se firma el [[./0_INF_BASE/PoC-DIP-001.org.pdf][*documento de inicio de proyecto]]* y se da paso a
la identificación de los distintos elementos clave de la investigación:

Actores clave

No.	Actores	Observaciones
1	Administrador	
2	Empleados con acceso al servidor	Disponen de cuentas con permiso de administración en el sistema
3	*Usuario ERP sospechoso*	Cuenta no controlada por el administrador. Se desconoce su origen.

Cuadro relacional

[[../2_INICIO/cuadro_relacional.png]]

Palabras clave

No.	Palabras clave	Observaciones
1	Sistema de ERP	Enterprise Resource Planning

|---|---|---|
2	Cuenta comprometida ERP	No se facilita la cuenta
3	Windows 2003	Sistema operativo del servidor comprometido
4	Actualizaciones del SO	El sistema se trataba de mantener actualizado
5	Cuentas privilegiadas	No se facilitan las cuentas Con permisos de administración Se utilizan para labores personales
6	Aplicaciones de usuario instaladas	No se especifican las aplicaciones

Activos clave

No.	Activos	Observaciones
1	Fichero	windows2003.img.gz

Croquis de escenario

No aplica.

Cadena de custodia

	Datos	Observaciones
Código	1	Ver PoC-IAI-001.pdf
Activo	{{{Activo_1}}}	Fichero comprimido
Hash	2f53bf2187ce9efcb1ec0e7f930141b36f2f7dc9	bash-3.2$ shasum -v 5.84
Fecha recopilación	[2015-06-14 Sun 10:59]	
Forma de recopil.	recolección	No se dispone de notario ni fedatario público.
Tamaño (bytes)	3500527266	El fichero descomprimido ocupa 5239471104 bytes
Número de copias	3 copias disponibles	1 en la web

| | | | 1 en servidor NAS |
			1 de trabajo
Responsable	{{{nomProf}}}		{{{cargoProf}}}

Documento de aceptación de fin de proyecto

Como final de la investigación se firmó el [[../0_INF_BASE/PoC-AAT-001.org.pdf][documento]] que acredita que la
misma se ha concluido satisfactoriamente y así se hace constar.

Observaciones finales

No ha habido [[../2_INICIO/PoC-RI-001.org][incidentes registrados]] a lo largo de la investigación.

\newpage

** Documentos de referencia

La documentación utilizada ha sido:

- Metodología de investigación informática forense en Emacs.
- http://resources.infosecinstitute.com/registry-forensics-regripper-command-line-linux/
- Documentación de otro participantes del reto.

\newpage

** Terminología y abreviaturas

- Información :: 'Todo conocimiento referido a un objeto o hecho, susceptible de codificación y almacenamiento.'
- Estados de la Información :: La información siempre debe estar codificada y por lo tanto siempre estará almacenada en algún sustento material. Este sustento puede encontrarse en uno de estos tres estados: Almacenamiento estático, almacenamiento dinámico, tránsito.
- Informática Forense :: conjunto multidisciplinario de teorías, técnicas y métodos de análisis, que brindan soporte conceptual y procedimental a la investigación de la prueba indiciaria informática.
- Prueba Informático Forense, características :: Se trata de una prueba pericial, basada en metodología criminalística, con fundamentos y características propias.
- Malware :: El término Malvare (Acrónimo en inglés de: 'Malcious software') engloba a todos aquellos programas 'maliciosos' (troyanos, virus, gusanos, etc.) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al

sistema informático o al usuario del mismo.
- Virus :: Código informático que se replica a sí mismo y se propaga de equipo en equipo por medio de programas o archivos a los que se adjunta. Para que se produzca la infección, es necesaria la intervención humana, es decir, el usuario debe realizar algún tipo acción como enviar un correo o abrir un archivo. Los virus pueden producir todo tipo de daños en el propio equipo y en la información y programas que éste contiene.

\newpage

** Proceso de análisis

El detalle del análisis se presenta en el documento [[../3_EVIDENCIAS/PoC-AIF-001.org][PoC-AIF-00

Entorno de trabajo

Para el análisis se ha instalado en una máquina virtual (2 procesadores, 2 Gb de RAM y 20 Gb de HD) que funciona sobre un MacBook Pro (4 procesadores, 16Gb de RAM y 500 Gb de HD) la distribución mini de Ubuntu 64bits sobre la que es posible desplegar el entorno forense de [[http://digital-forensics.sans.or [[http://lxde.org/es][LXDE]] como entorno de escritorio X11 liviano, [[http://www.gnu.org/softwar herramienta que se requiera.

En el contexto descrito se ha instalado una máquina virtual con los siguientes paquetes:

- ENTORNO Linux
  - [X] VM SIFT (Sans Forensics)
+ http://sift.readthedocs.org/en/latest/packages/index.html#all-packages
+ sleuthkit/Autopsy
+ mac-robber
+ mactime
+ dcfldd
+ dc3dd
+ tcpdump
+ wireshark
+ [[http://plaso.kiddaland.net/usage][Plaso]]
+ [[http://www.forensicswiki.org/wiki/Bulk_extractor#Download][bulk_extractor]]
  - http://www.dragonjar.org/data-carvers-en-retos-forenses.xhtml
  - http://www.dragonjar.org/bulk-extractor.xhtml
+ libqcow-tools
+ libsmdev-tools
+ libsmraw-tools
+ libvhdi-tools
+ libvmdk-tools
  - [X] Emacs 24
  - [X] tmux

  - [X] parcellite/glipper/klipper/
  - [X] sshfs
  - [X] autofs
  - [X] memdump
  - [X] [[https://code.google.com/p/lime-forensics][lime forensics]]

Se ha creado el siguiente usuario:

- Usuario: investigador
- Contraseña: forense

Se ha generado el par de claves para el usuario ~Investigador Forense~, con dirección de correo inventada ~investigador@forense.fi.upm.es~:

#+BEGIN_QUOTE
investigador@EFI:~$ gpg --edit-key 29678D06
gpg (GnuPG) 1.4.16; Copyright (C) 2013 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Clave secreta disponible.

pub 2048R/29678D06 creado: 2015-05-26 [caduca: nunca   ] uso: SC
                     confianza: absoluta   validez: absoluta
sub 2048R/DAC61BAB creado: 2015-05-26 [caduca: nunca   ] uso: E
[absoluta] (1). Investigador Forense (Cifrado de información crítica de proyectos forenses digitales) <investigador@forense.fi.upm.es>
#+END_QUOTE

Para el acceso a la imagen forense se monta una unidad compartida donde se encuentra el fichero de imagen.

Actuaciones

- Se chequea la integridad del fichero de imagen a analizar.

- Se ejecuta una herramienta (bulk-extractor) de extracción de información del fichero de imagen.

- Identificación del sistema de ficheros de la evidencia.

  + No me planteo arrancar el sistema por el propio planteamiento del PFC de utilizar exclusivamente Emacs.

- Montar en ~modo de sólo lectura~ el fichero de imagen objeto del análisis.

- Líneas de tiempo de los ficheros de la imagen

  + He utilizado [[http://www.sleuthkit.org/mac-robber/index.php][mac-robber]] para recoger toda
    los ficheros del sistema analizado y se puede ver las salida en el
    fichero [[./poc_mac_robber.mac]].

    A continuación se utiliza [[http://wiki.sleuthkit.org/index.php?
    title%3DMactime][mactime]] para dar un formato más
    comprensible al contenido obtenido en el paso anterior y se puede
    ver el resultado en el fichero [[./poc_mactime.txt]].

- Configuración de las tarjetas de red

  + Se observa que la dirección IP es fija (192.168.5.5/24) y no está
    configurado el DHCP.

    #+BEGIN_EXAMPLE
    /media/investigador/WINDOWS/system32/config $
    Launching nic v.20100401
    nic v.20100401
    (System) Gets NIC info from System hive

    Adapter: {44C3A521-98D1-4B7A-850D-860BB2324A1D}
    LastWrite Time: Thu Jan 26 06:26:22 2006 Z
      EnableDHCP   1
      IPAddress   0.0.0.0
      SubnetMask   0.0.0.0
      DefaultGateway

    Adapter: {5269ADEB-9E6D-4673-B898-4238F085972C}
    LastWrite Time: Thu Jan 26 06:26:22 2006 Z
      EnableDHCP   0
      IPAddress   192.168.5.5
      SubnetMask   255.255.255.0
      DefaultGateway   192.168.5.254
      DhcpIPAddress   0.0.0.0
      DhcpSubnetMask   255.0.0.0
      DhcpServer   255.255.255.255
      Lease   3600
      LeaseObtainedTime   Sun Jan 29 01:18:17 2006 Z
      T1   Sun Jan 29 01:48:17 2006 Z
      T2   Sun Jan 29 02:10:47 2006 Z
      LeaseTerminatesTime Sun Jan 29 02:18:17 2006 Z
    #+END_EXAMPLE

- Exportación de los ficheros de eventos de windows ~evt~.

  + Utilizando la herramienta ~[[http://manned.org/evtexport/7573a4f8]
    [evtexport]]~ se obtiene el contenido de los
    ficheros:

* AppEvent.Evt
* SecEvent.Evt
* DnsEvent.Evt
* SysEvent.Evt

- Obtencion de la lista preliminar de ficheros.

  + He utilizado [[http://www.sleuthkit.org/mac-robber/index.php]
    [mac-robber]] para recoger toda la información relativa a
    los ficheros del sistema analizado. Se puede ver las salida en el
    fichero [[../3_EVIDENCIAS/poc_mac_robber.mac][poc_mac_robber]].

  + A continuación se utiliza [[http://wiki.sleuthkit.org/index.php?
    title%3DMactime][mactime]] para dar un formato más
    comprensible al contenido obtenido en el paso anterior:Y se puede
    ver el resultado en el fichero [[../3_EVIDENCIAS/poc_mactime.txt][poc_mactime]].

- Información de usuarios y grupos del sistema.

- Obtención de las contraseñas de usuario.

  + Dado que no se va a acceder al sistema no se trata de una tarea
    imprescindible, pero si es necesario acceder se dispondrá de las
    mismas.

  + Para obtener el fichero con los hashes de los usuarios (de la
    [[https://en.wikipedia.org/wiki/Security_Account_Manager][SAM)]]
    hay que obtener el ~Syskey~ ([[https://en.wikipedia.org/wiki/Syskey]
    [System key]]), y finalmente crackear los
    hashes para determinar las contraseñas de los usuarios.

    Una vez obtenido el fichero con los hashes, utilizamos ~John the
    ripper~ para obtener las contraseñas, como se puede ver a
    continuación:

    #+BEGIN_EXAMPLE
    Loaded 37 password hashes with no different salts (LM [DES 128/128 SSE2-16])
    Press 'q' or Ctrl-C to abort, almost any other key for status
    MORA   (zamorano:2)
    P0STGR3   (postgres:1)
    R3N0   (reno:2)
    PASSWOR   (ver0k:1)
                     (SUPPORT_388945a0)
                     (Guest)
    1   (mpenelope:2)
    2000   (moni:2)
    CARMEN8   (amado:1)
    D   (ver0k:2)
    4   (lalo:2)

```
R                (ernesto:2)
LY               (pili:2)
3                (mirna:2)
3                (amado:2)
18               (maick:2)
JUANG11          (maick:1)
MELUCHA          (maru:1)
30               (caracheo:2)
83               (katy:2)
RODOLFO          (reno:1)
MMONICA          (moni:1)
026              (maru:2)
LALOLOC          (ovejas:1)
O86              (ovejas:2)
TEGUIZA          (zamorano:1)
CHIRIPI          (pili:1)
CHLN026          (katy:1)
MIRK4AR          (mirna:1)
T3R3CLT          (lalo:1)
T3MP0RA          (mpenelope:1)
T3WPJ0H          (Johnatan)
SSQL             (postgres:2)
3RN3S70          (ernesto:1)
L,               (Administrator:2)
U7R3$7U          (Administrator:1)
C4R$4CH          (caracheo:1)
37g 0:02:51:36 3/3 0.003593g/s 45521Kp/s 45521Kc/s 90542KC/s C4R$4BU..C4R$4DW
Warning: passwords printed above might be partial
Use the '--show' option to display all of the cracked passwords reliably
Session completed
~ $
#+END_EXAMPLE
```

A continuación se presenta un listado con el formato
~USUARIO:CONTRASEÑA:ID:resto~

```
#+BEGIN_EXAMPLE
Administrator:U7R3$7UL,:500:fad82559a3669bf1c349641028e9bf3b:ecde6a92576ca84b5ddcd7cb117bab50
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0::1001:aad3b435b51404eeaad3b435b51404ee:8dcca3eb5e2ed3503e483df0dce5f072:::
Johnatan:T3WPJ0H:1006:fbc89204579fc565aad3b435b51404ee:7750def414475cf2b9b45a64fdd3481a:::
ernesto:3RN3S70R:1007:aa4d59741693011a944e2df489a880e4:2c759a0f3165fe70f3b2ef1355dbbf4e:::
amado:CARMEN83:1008:59cbc5117eaef5c21aa818381e4e281b:0ade3431a00b403ccc562b6cf629ab77:::
maick:JUANG1118:1009:85fec305e34929d18347bb1e72cc9f76:0e13f8a840ea89fcd88cb36b962a2f14:::
lalo:T3R3CLT4:1010:3264cf6b06490f7cff17365faf1ffe89:10ee4264b00cc787b80f6f3c80dcf9c5:::
moni:MMONICA2000:1011:506b60f26bb9aeef8b4c5fc57ce52905:0ac8ae6ef8beaae7c61cf4230c7a3b8d:::
maru:MELUCHA026:1012:03fb789ef35a2b6d40967f66e935e1ff:2e4f31fe3248f2bc9d1e961b579f0e5f:::
mirna:MIRK4AR3:1013:4547b34ebb1a63e81aa818381e4e281b:b84ef18830b2b30ba60105d507eaaec9:::
katy:CHLN02683:1014:b487217fce8da54ddc0adaac127d3673:2ce609fe8387032f3c7fbbfc7f4bd931:::
```

```
caracheo:C4R$4CH30:1015:10972d878c8158d23830ab41f50b8c79:1f29efc37cc7c33148c3b1a16b81c45
ovejas:LALOLOCO86:1016:36cea0da9720c1866f3baf47315038ff:16fb5c5803db901b39f38adcfda64bf7
reno:RODOLFOR3N0:1017:f903d899f9f2f54138e225910e5ac3d2:da8ffa76f679c3a79d46b96d61758f34:
pili:CHIRIPILY:1018:7ed41ffdc962e828527c3e14a6132a0f:8963676b5ef71347321fca96dfcf2243:::
zamorano:TEGUIZAMORA:1019:4f11278e04ff02b3451e935871f3e930:5550a4a120a88cfc12e1c856344d9
mpenelope:T3MP0RA1:1020:7d536e187e4a5a05c2265b23734e0dac:2a6f455e8094160b511a810e4e8aee6
postgres:P0STGR3SSQL:1023:c848af05f3d8ca3c929ca03322bf4367:6812a8dcfcad8c09a65696fa3e893
ver0k:PASSWORD:1024:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::

37 password hashes cracked, 0 left
#+END_EXAMPLE
```

- Búsqueda de virus o malware.

  + Se ejecuta [[http://www.clamav.net/index.html][ClamAV]] y se identifica el fichero ~explorer.exe~ en el directorio ~My Documents~ del usuario ~Administrator~ infectado por ~Win.Trojan.Clons-725~.

- Exportación de ficheros ~evt~.

  + Se observa que el sistema fue inicialmente configurado con la hora de Alaska, y no fue hasta el dia 2 de Febrero cuando se cambio a la hora estandar PST.

  + Se pueden observar las fechas de creación de los diferentes usuarios, lo que

- Análisis de logs de aplicaciones.

  + C:\apache\Apache\logs

  + C:\apache\Apache\mysql\data\

  + C:\Program Files\PostgreSQL\8.1\data\pg_log

- Se ha identificado software de seguridad para el uso del administrador en ~C:\Documents & Settings\Administrator\My Documents\Sof7w4r3~

  + [[http://www.nirsoft.net/utils/cports.html][CurrPorts v.1.07]], una utilidad para listar los puertos TCP y UDP abiertos en el sistema.
  + TCPView 2.40, una utilidad de www.sysinternals.com con el mismo proposito que la anterior.
  + GFI LANguard Network Security Scanner v6.0, que aunque presente no llego a instalarse en el sistema.

- Se analiza el ~profile~

  + Aquí podemos ver que no todos los perfiles de usuario han estado
    activos hasta el momento del apagado del sistema, y de echo algunos
    apenas han tenido actividad desde el momento de su creación, por lo
    que se puede descartar a la hora del análisis.

  + Los usuarios activos en los momentos previos al apagado son,
    ~Johnatan~, ~ver0k~ y ~Administrator~.

- Información de usuarios y grupos del sistema

  + Aquí obtenemos información adicional que es interesante, como el
    número de veces que los usuarios han accedido al sistema y que nos
    permite descartar a muchos usuarios.

    Por otro lado, el usuario ~ver0k~ es el único que apenas está
    cumplimentado. No tiene nombre ni descripción y fué creado el mismo
    día que se apaga el servidor, pero unas horas antes, lo que implica
    que es un vector de investigación muy claro.

- Análisis de tiempos en usuarios y grupos del sistema

  + Con el objetivo de desarrollar un TLN (Time Line analisis) lo más
concreto posible se obtienen datos relativos a eventos concretos de los
distintos usuarios, como la creación de la cuenta o el último acceso de
los usuarios.

  + Organizando esta información podríamos observar situaciones interesantes
a la hora de realizar el análisis como una posible relación entre la
actividad de los usuarios ~Johnatan~ y ~ver0k~.

- Análisis de MSN

  + A raíz de identificar que el Administración instaló la herramienta MSN
    se ha visto que el único usuario que lo utilizó es ~ver0k~.

  + Se analiza la información que encontramos una serie de ficheros
    temporales bajo ~C:\Documents and Settings\ver0k\Application
    Data\Microsoft\MSN Messenger\3817870080~, donde este ultimo numero es el
    UserID generado a partir del nombre del usuario.

    Aunque no es posible obtener el nombre de usuario a partir del UserID,
    si es posible comprobar si una determinada direccion de correo genera
    ese mismo UserID.

    Dado que entre la información recabada por bulk-extractor hay una serie
    de direcciones de correo obtenidas mediante el procedimiento de file
    carving, se desarrolló un programa para generar el UserID de todos los
    casos obteniendo un match: ~h4ckIII@hotmail.com~, lo que nos confirma
    que fue esta la cuenta empleada por el atacante.

Adicionalmente se confirma ademas por el hecho de encontrar en el fichero

~C:\Documents and Settings\ver0k\NTUSER.DAT~ la siguiente entrada: ~Software\Microsoft\CurrentVersion\UnreadMail\h4ckIII@hotmail.com~

Buscando la cadena ~h4ckIII~ en los resultados de bulk-extractor y accediendo a posiciones de memoria concretas de la imagen se obtiene información referente a otra dirección ~h4ckiii-2@hotmail.com~.

#+BEGIN_EXAMPLE
INVITE MSNMSGR:h4ckiii-2@hotmail.com MSNSLP/1.0
To: <msnmsgr:h4ckiii-2@hotmail.com>
#+END_EXAMPLE

+ Se sospecha que esta es la vía por la que se ha podido sacar información si bien no se tienen evidencias de tal actividad.

Análisis

Del análisis, fundamentado en buenas prácticas o experiencias previas, de los distintos artefactos se obtiene la información que se presenta a continuación.

Para toda aquella información que sea demasiado extensa o técnica se puede consultar en el documento [[../3_EVIDENCIAS/PoC-AIF-001.org][PoC-AIF-001]] facilitado.

- Fecha de instalación del equipo

  + El resultado obtenido tras acceder a ~Microsoft\Windows NT\CurrentVersion~ y listar las claves, se observa el valor de la clave ~InstallDate~:

    #+BEGIN_EXAMPLE
    4 REG_DWORD   <InstallDate>   1138258604 [0x43d872ac]
    #+END_EXAMPLE

    El dato facilitado son los segundos transcurridos desde el 1 de enero de 1970, y para conocer la fecha y hora concreta debe de realizarse el correspondiente cálculo.

    Sumando 1138258604 segundos al 1/1/1970 obtenemos ~Thu, 26 Jan 2006 06:56:44 GMT~.

- Determinacion del huso horario

  + DaylightName   -> Pacific Daylight Time

+ StandardName   -> Pacific Standard Time

- Sistema operativo

  + Los resultados obtenidos son:

    #+BEGIN_EXAMPLE
    > cat Microsoft\Windows NT\CurrentVersion\ProductName
    Value <Microsoft\Windows NT\CurrentVersion\ProductName> of type REG_SZ, data length 66 [0x42]
    Microsoft Windows Server 2003 R2

    > cat Microsoft\Windows NT\CurrentVersion\CSDVersion
    Value <Microsoft\Windows NT\CurrentVersion\CSDVersion> of type REG_SZ, data length 30 [0x1e]
    Service Pack 1
    #+END_EXAMPLE

- Obtención del listado de usuarios

  + Mediante una herramienta que automatiza la búsqueda se obtienen los
    usuarios del sistema.

    #+BEGIN_EXAMPLE
    Loaded hives: <SAM><software>

      1 - Edit user data and passwords
      3 - RecoveryConsole settings
      4 - Show product key (DigitalProductID)
          - - -
      9 - Registry editor, now with full write support!
      q - Quit (you will be asked if there is something to save)

    What to do? [1] -> 1

    ===== chntpw Edit User Info & Passwords ====

    | RID -|---------- Username ------------| Admin? |- Lock? --|
    | 01f4 | Administrator | ADMIN | |
    | 03f0 | amado | | |
    | 03f7 | caracheo | | |
    | 03ef | ernesto | ADMIN | |
    | 01f5 | Guest | | dis/lock |
    | 03ee | Johnatan | ADMIN | |
    | 03f6 | katy | | |
    | 03f2 | lalo | | |
    | 03f1 | maick | | |
    | 03f4 | maru | ADMIN | |

```
    | 03f5 | mirna                          |        |          |
    | 03f3 | moni                           |        |          |
    | 03fc | mpenelope                      |        | dis/lock |
    | 03f8 | ovejas                         |        |          |
    | 03fa | pili                           |        |          |
    | 03ff | postgres                       |        |          |
    | 03f9 | reno                           |        |          |
    | 03e9 | SUPPORT_388945a0               |        | dis/lock |
    | 0400 | ver0k                          | ADMIN  |          |
    | 03fb | zamorano                       |        |          |

    Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
    or simply enter the username to change: [Administrator] !

    #+END_EXAMPLE
```

- Hora del último apagado

  + ShutdownTime = Sun Feb 5 23:44:32 2006 (UTC)

- Sofware Instalado

  La lista del software instalado en el sistema es la siguiente:

  + Apache HTTP Server 1.3.34
  + Mozilla Firefox (1.5.0.1)
  + MSN Messenger 7.5
  + MySQL Administrator 1.1
  + MySQL Server 4.1
  + PHP 4.4.2
  + PostgreSQL 8.1
  + Hotfixes KB896422, KB896424, KB896428, KB896358, KB896727, KB899587, KB899589, KB901017,KB901214, KB902400, KB903235, KB905414, KB908519, KB890046 y KB896688.

- Configuración del firewall

  + El analisis de los puertos TCP y UDP abiertos en el sistema indica que el puerto 3389 asociado al servicio de Terminal Server está accesible, lo que podría por un vector de entrada para un atacante.

  + Podemos ver que el firewall del servidor está activo, y los puertos abiertos (y no nateados) son:

* 445:TCP -> 445:TCP
* 2869:TCP -> 2869:TCP
* 5432:TCP -> 5432:TCP
* 138:UDP -> 138:UDP
* 139:TCP -> 139:TCP

* 3389:TCP -> 3389:TCP
* 137:UDP -> 137:UDP
* 1900:UDP -> 1900:UDP

- Terminal Server

  + Se verifica que el servicio de Terminal Server estaba habilitado.

- Unidades compartidas

  + No se han identificado unidades compartidas.

- Busqueda de 'malware'.

  + Se verifica que no se ha activado el ~Malicious Software Removal
    Tool~.

- Documentos recientes accedidos por los usuarios

  + Analizando estos documentos y el momento en el que se dan parece
    claro que el usuario ~ver0k~ tiene un comportamiento sospechoso por
    el volumen de ficheros consultados en muy corto tiempo y el tipo de
    los mismos.

    #+BEGIN_EXAMPLE
    Launching recentdocs v.20100405
    recentdocs v.20100405
    (NTUSER.DAT) Gets contents of user's RecentDocs key

    RecentDocs
    **All values printed in MRUList\MRUListEx order.
    Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
    LastWrite Time Sun Feb 5 21:58:56 2006 (UTC)
      18 = Administrator's Documents
      37 = examen.gif
      36 = Apache
      35 = ABOUT_APACHE.TXT
      34 = maick
      33 = Sti_Trace.log
      32 = RRGEPPortadas.doc
      31 = RRGEPNotas.doc
      30 = Notas.doc
      24 = Indice Pormenorizado.doc
      29 = ÍNDICE DOCTORADO.doc
      28 = formulario.doc
      23 = 30SEP_bolecart-book.doc
      26 = Israel Robledo Gonzáles's Documents
      27 = concha.doc
      25 = Boletin11.doc

```
  19 = modelos
  22 = nm06082003.jpeg
  21 = nm06052003.jpeg
  20 = nm06042003.jpeg
  10 = nm06032003.jpeg
  9 = a017.jpg
  7 = imagenes
  8 = overlay_por_2006020110007_20060201224249.jpg
  6 = overlay_por_2006020107034_20060201190204.jpg
  17 = overlay_9_2006020110006.jpg
  16 = overlay_8_2006020110005.jpg
  15 = overlay_8.jpg
  14 = overlay_7_2006020110005.jpg
  13 = overlay_6_2006020110004.jpg
  12 = overlay_6_2005112211035.jpg
  11 = overlay_5_2006020110004.jpg
  4 = Local Disk (C:)
  5 = users.txt
  3 = clientes.txt
  1 = web-erp
  2 = config.php
  0 = AccountGroups.php

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.doc
LastWrite Time Sun Feb  5 21:47:42 2006 (UTC)
MRUListEx = 8,7,1,6,5,4,0,3,2
  8 = RRGEPPortadas.doc
  7 = RRGEPNotas.doc
  1 = Notas.doc
  6 = Indice Pormenorizado.doc
  5 = ÍNDICE DOCTORADO.doc
  4 = formulario.doc
  0 = 30SEP_bolecart-book.doc
  3 = concha.doc
  2 = Boletin11.doc

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.gif
LastWrite Time Sun Feb  5 21:58:55 2006 (UTC)
MRUListEx = 0
  0 = examen.gif

Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpeg
LastWrite Time Sun Feb  5 21:19:05 2006 (UTC)
MRUListEx = 3,2,1,0
  3 = nm06082003.jpeg
  2 = nm06052003.jpeg
  1 = nm06042003.jpeg
  0 = nm06032003.jpeg
```

```
    Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.jpg
    LastWrite Time Sun Feb  5 21:18:05 2006 (UTC)
    MRUListEx = 4,3,2,1,0,9,8,7,6,5
      4 = a017.jpg
      3 = overlay_por_2006020110007_20060201224249.jpg
      2 = overlay_por_2006020107034_20060201190204.jpg
      1 = overlay_9_2006020110006.jpg
      0 = overlay_8_2006020110005.jpg
      9 = overlay_8.jpg
      8 = overlay_7_2006020110005.jpg
      7 = overlay_6_2006020110004.jpg
      6 = overlay_6_2005112211035.jpg
      5 = overlay_5_2006020110004.jpg

    Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log
    LastWrite Time Sun Feb  5 21:49:52 2006 (UTC)
    MRUListEx = 0
      0 = Sti_Trace.log

    Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.php
    LastWrite Time Sun Feb  5 20:50:02 2006 (UTC)
    MRUListEx = 1,0
      1 = config.php
      0 = AccountGroups.php

    Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.txt
    LastWrite Time Sun Feb  5 21:53:46 2006 (UTC)
    MRUListEx = 2,1,0
      2 = ABOUT_APACHE.TXT
      1 = users.txt
      0 = clientes.txt

    Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\Folder
    LastWrite Time Sun Feb  5 21:58:56 2006 (UTC)
    MRUListEx = 8,7,2,6,5,3,1,0
      8 = Administrator's Documents
      7 = Apache
      2 = maick
      6 = Israel Robledo Gonzáles's Documents
      5 = modelos
      3 = imagenes
      1 = Local Disk (C:)
      0 = web-erp
    #+END_EXAMPLE

- URLs accedidas

  + Analizando las URLs accedidas por los usuarios hay dos usuarios que
    llaman la atención:
```

* Vemos que el ~Administrator~ ha accedido a google, a la unidad de
      disco (C:) y se ha descargado la herramienta de IM de
      Microsoft. Sin embargo este usuario no ha accedido con ningún
      usuario ya que el directorio ~C:/Documents and
      Settings/Administrator/Application Data/Microsoft/MSN Messenger~
      aparece vacío.

* Vemos que ~Johnatan~ ha accedido a google, al correo de yahoo y
      seguidamente al ERP.

\newpage

** Cronología de eventos

A continuacion se presenta un sumario del cronograma de las actividades
mas destacables detectadas en el sistema, junto con la evidencia
asociada.

Para el analisis temporal he intentado siempre corroborar cualquier
hipotesis desde varias fuentes, si bien por razones de espacio, se
muestran las evidencias de forma abreviada.

Asimismo, todas las horas estan referidas al huso horario del Pacifico
(PST, o GMT-8) aunque la evidencia en ocasiones este asociada a GMT o
Alaska (GMT-9), como ya he comentado.

- ~Thu, 26 Jan 2006 06:56:44 GMT~: Se instala el sistema operativo.

  + Entrada del registry HKLM\Software\Microsoft\Windows\CurrentVersion\InstallDate: 0x43d87

- ~26-ene-06 18:00~: Instalación de Apache.

  + Tiempo de creacion de los directorios C:\apache, y los directorios
    bin, lib, conf, etc.. bajo C:\apache\Apache

- ~26-ene-06 18:39~: Instalación de MySQL

  + Tiempo de creacion de los directorios bin, lib, etc.. bajo
    C:\apache\Apache\mysql.

- ~26-ene-06 18:47~: Instalación de WebERP.

  + Tiempo de creacion del directorio C:\apache\Apache\htdocs\web-erp.

- ~29-ene-06 18:01~: Se hace una primera prueba externa de seguridad del
  servidor web, que deja una curiosa entrada en el log:

  + Apache error log: Sun Jan 29 17:01:43 134.186.42.18 client sent

HTTP/1.1 request without hostname (see RFC2616 section 14.23):
/w00tw00t.at.ISC.SANS.DFi
(v. http://isc.sans.org/diary.php?storyid=900)

- ~30-ene-06 18:28:30 a 18:31:43~: Escaneo de vulnerabilidades del servidor apache desde la direccion IP 192.168.100.144 (dentro pues de la red privada) con la herramienta 'nikto'.

  + Entradas en el Apache error log: Mon Jan 30 17:28:30 [error] 192.168.100.144 File does not exist: c:/apache/apache/htdocs/nikto-1.35-d3ng4mwwxva0fqq8.htm

- ~30-ene-06 18:28:34~: Intento de ataque singular desde 132.248.124.144, buscando un problema conocido con cgi-bin/excite, sin consecuencias.

  + Apache error log Mon Jan 30 17:28:34 132.248.124.144 request failed: erroneous characters after protocol string: GET /cgi-bin/excite;IFS=\\\\\\'$\\\\\\';

- ~1-feb-06 18:53:00 a 18:53:45~: Otro escaneo con nikto, esta vez desde 192.168.5.32

  + Apache error log:

* Wed Feb 01 17:53:03 192.168.5.32 File does not exist: c:/apache/apache/htdocs/nikto-1.35-hrzububfwsfi.htm

* Wed Feb 01 17:53:45 192.168.5.32 (2)No such file or directory: script not found or unable to stat: c:/apache/apache/cgi-bin/where.pl

- ~2-feb-06 12:59:57~: Se pone como nuevo 'timezone' la hora estandar del Pacifico (PST)

  + System EventLog: 02/02/2006 12:59:57 ; ; ; ; 428323; 60; 480 Pacific Standard Time;

- ~2-feb-06 18:34:18 a 18:45:35~: El usuario 'reno' copia 514 ficheros bajo C:\Documents and Settings en los directorios de distintos usuarios incluyendo ficheros Excel, Word, presentaciones Powerpoint, PDFs e imagenes pornograficas en formato 'jpg'.

  + Evidencias asociadas: Security Event Log: Account Used for Logon by reno 02/02/2006 18:34:18 Tiempo de creacion de los distintos ficheros creados, junto con el propietario de los mismos (el usuario reno es el unico que tiene todos los permisos).

  + En total, se copian 173.079.187 bytes en 11 minutos y 17 segundos, lo que nos permite deducir que la velocidad de conexion para la copia fue de 2Mbits.

- ~4-feb-06 14:04:43 a 14:26:54~: Escaneo de vulnerabilidades del servidor web desde 84.18.17.15. En esta ocasion si que parece un ataque real, por cuanto es una IP externa y no se usa 'nikto'.

  + Apache error log Sat Feb 04 14:04:43 84.18.17.15 Invalid method in request \\x80.\\x01

- ~4-feb-06 14:19:14 a 14:19:19~: ataque tipo denegacion de servicio desde 4.18.17.15.

  + Apache error log Sat Feb 04 14:19:14 4.18.17.15 (38)Filename too long: Possible DoS attempt? Path=c:/apache/apache/htdocs/////////////////////////// (unas 300 lineas iguales)

- ~4-feb-06 14:45:44 a 14:47:07~: Instalacion de PostgreSQL.

  + File Access 04/02/2006 14:45:44 C\Program Files\PostgreSQL\8.1\bin\libpq.dll
  + Sec Event Log 04/02/2006 14:46:23 Se crea la cuenta del usuario postgres

- ~4-ene-06 14:47:30~: El administrador crea el directorio C:\Documents and settings\Administrator\Sof7w4r3

  + File Creation Sof7w4r3 14:47:30

- ~4-ene-06 14:59:43~: copia dentro los ficheros Tcpview.exe, languardnss6.exe y cports.exe.

  + Tiempo de creacion de los ficheros.

- ~4-feb-06 15:28:25~: El administrador genera el directorio Crea el directorio C:\Documents and Settings\Administrator\My Documents\update que contiene algunos hotfixes a instalar.

  + File creation:

* updates 15:28:25

* Blaster Windows2000-KB823980-x86-ESN.exe 15:28:25

* Buffer Overrun Windows2000-KB824146-x86-ESN.exe 15:28:26

* Netbios Windows2000-KB824105-x86-ESN.exe 15:28:27

* w2k ntdll iis.EXE 15:28:27

* Windows2000-KB828741-x86-ESN.EXE 15:28:27

* Windows2000-KB835732-x86-ESN.EXE 15:28:32

- ~5-feb-06 12:11:13~: Comienzo del ataque. Alguien, en algún lugar, crea un correo con el que intenta conseguir que un usuario del sistema (Johnatan) acceda a una URL determinada, mediante la cual tiene previsto conseguir acceso al sistema.

  + Analizando los indicios obtenidos mediante bulk-extractor se ha recuperado el siguiente e-mail. Se trata de un correo tipo 'phishing' en el que intenta enganar a Johnatan, haciendose pasar por alguien por el conocido (Alberto Lopez) para darle confianza.

    #+BEGIN_EXAMPLE
    De: alopez@eycsa.com.mx
    Para: jonathan.tezca@yahoo.com
    Asunto: Urgente!!
    Fecha: Sun, 5 Feb 2006 14:11:13 -0600 (CST)
    Johnny:
    Por favor baja el catalogo que esta en http://70.107.249.150/clientes.wmf
    Alberto Lopez
    Director General
    Electronica y Computacion S.A. de C.V.
    #+END_EXAMPLE

- ~5-feb-06 12:23:09~: El usuario Johnatan hace login en el sistema. Es particularmente importante porque es este usuario y en esta sesion el que va a sufrir el ataque.

  + Security Event Log 05/02/2006 12:23:09 Successful Logon -- Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A); Method - Logon Occurred on This Machine; Logon Process - User32 ; Authentication Package - Negotiate; Workstation - COUNTERS; - -;

- ~5-feb-06 12:23:49~: Johnatan arranca el Internet Explorer. (con Process ID 3128)

  + Security Event Log 05/02/2006 12:23:49 New Process Has Been Created -- New Process ID - 3128; Image File Name - C:\Program Files\Internet Explorer\IEXPLORE.EXE; Creator Process ID Domain - 904; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

- ~5-feb-06 12:26:46~: Johnatan se conecta a mail.yahoo.com. para leer su correo.

  + De Documents and Settings\Johnatan\Local Settings\History\History.IE5\index.dat:: 05/02/2006 12:26:46 Link :2006020520060206: Johnatan@http://mail.yahoo.com

- ~5-feb-06 12:41:30~: Primer intento de ataque. Johnatan ha caido en la trampa y accede a http://70.107.249.150/clientes.wmf. Sin embargo, el

exploit falla y no hayconsecuencias aparentes.

+ index.dat 05/02/2006 12:41:30 Link Visited: Johnatan@http://70.107.249.150/clientes.wmf

- ~5-feb-06 12:43:44~: Johnatan abre otro correo

+ index.dat: 05/02/2006 12:43:44 Link Visited:
Johnatan@http://e1.f376.mail.yahoo.com/ym/ShowLetter?MsgId=6084_0_553_1161_187_0_4_-
1_0_oSOYkYn4Ur6Rg9SuJfSMZylawvafl_ZIeGfzYTPKxPtBv1w5lalEg_wancdKNiXSzdaV.JLnI3Unfrc9E7gE
kyR

- ~5-feb-06 12:43:50~: Internet explorer advierte a Johnatan de que el contenido ha sido bloqueado. Pero este ignora la advertencia y sigue adelante.

+ File Access 05/02/2006 12:43:50 Windows XP Pop-up Blocked.wav

- ~5-feb-06 12:44:10~: Se accede a http://70.107.249.150:8080/clientes.wmf

+ index.dat 05/02/2006 12:44:10 Link Visited:
Johnatan@http://70.107.249.150:8080/clientes.wmf

- ~5-feb-06 12:44:11~: ¡¡¡EXPLOIT!!! El atacante arranca un interprete de comandos en el sistema accesible desde el exterior. Ademas, como Johnatan pertenece al grupo Administrators, con privilegios de Administrador.

+ Arranca el proceso cmd.exe 3376, PPID 884 (run32dll32.exe, hijo a su vez de 3128, el internet explorer de Johnatan)

Iexplorer index.dat 05/02/2006 12:44:11 Link Visited: Johnatan@
http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJ0KMsfYBZnaFKx6dZs
/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU5Oi/AUWWckI2mU/LQ9ClubslAJKIa2jdYtSFExez4sRyL.tiff

Sec Event Log 05/02/2006 12:44:11 New Process Has Been Created -- New Process ID - 884; Image File Name - C:\WINDOWS\system32\rundll32.exe; Creator Process ID Domain - 3128; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

Sec Event Log 05/02/2006 12:44:12 New Process Has Been Created -- New Process ID - 3376; Image File Name - C:\WINDOWS\system32\cmd.exe; Creator Process ID Domain - 884; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

La vulnerabilidad aprovechada se basa en un mal tratamiento de los ficheros WMF yesta descrita en el boletin :
http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx

El exploit empleado es uno disponible dentro del Framework de Metasploit

http://www.metasploit.com/projects/Framework/exploits.html#ie_xp_pfv_metafile

El cual aprovecha un 'bug' en la function 'Escape' para ejecutar codigo arbitrario a traves del procedimiento SetAbortProc de la libreria GDI. Ademas, el exploit genera una URL random y un fichero .tif tambien random que contiene el exploit, para evitar las firmas de los IDS.

El empleo de este exploit o uno muy similar puede confiirmarse por la URL a la que es direccionado Johnatan para acceder al stream WMF:
http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJ0KMsfYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU5Oi/AUWWckI2mU/LQ9ClubslAJKIa2jdYtSFExez4sRyL.tiff

Y por la existencia de dicho fichero .tif entre los que son recuperables dentro de los ficheros temporales de Internet. En concreto, lo encontramos en C:\Documents and Settings\Johnatan\Local Settings\Temporary Internet Files\Content.IE5\LQ9ClubsIAJKIa2jdYtSFExez4sRyL.tiff.

- ~5-feb-06 12:45:30~: El atacante anade la cuenta ver0k, con 'net user ver0k password /ADD'.

  + El password empleado es precisamente 'password', averiguado al 'crackear' las cuentas.

  + Notese que el Creator Process ID es 3376, correspondiente al proceso cmd.exe. Security Event Log:

    * 05/02/2006 12:45:30 New Process Has Been Created -- New Process ID - 2988; Image File Name - C:\WINDOWS\system32\net.exe; Creator Process ID Domain - 3376; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

    * 05/02/2006 12:45:30 New Process Has Been Created -- New Process ID - 3700; Image File Name - C:\WINDOWS\system32\net1.exe; Creator Process ID Domain - 2988; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

    * 05/02/2006 12:45:30 User Account Created -- New Account Name - ver0k; New Domain - COUNTERS; New Account ID - %{S-1-5-21-2780117151-1340924567-2512508698-1024}; Caller User Name - Johnatan; Caller Domain - COUNTERS; Caller Logon ID - (0x0,0x3DF69A); Privileges - -; - ver0k;

    * 05/02/2006 12:45:30 User Account Password Set -- Target Account Name - ver0k; Target Domain - COUNTERS; Target Account ID - %{S-1-5-21-2780117151-1340924567-2512508698-1024}; Caller User Name - Johnatan; Caller Domain - COUNTERS; Caller Logon ID - (0x0,0x3DF69A); - -;

- ~5-feb-06 12:45:53~: Luego anade la cuenta ver0k al grupo Administrators, con el comando 'net group 'Administrators' ver0k /ADA'

  + Security Event Log:

    * 05/02/2006 12:45:53 New Process Has Been Created -- New Process ID - 2744; Image File Name - C:\WINDOWS\system32\net.exe; Creator Process ID Domain - 3376; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

    * 05/02/2006 12:45:53 New Process Has Been Created -- New Process ID - 2576; Image File Name - C:\WINDOWS\system32\net1.exe; Creator Process ID Domain - 2744; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

    * 05/02/2006 12:45:53 Local Group Member Added -- Member - -; Target Account Name - %{S-1-5-21- 2780117151-1340924567-2512508698-1024}; Target Domain - Administrators; Target Account ID - Builtin; Caller User Name - %{S-1-5-32-544}; Caller Domain - Johnatan; Caller Logon ID - COUNTERS; Privileges - (0x0,0x3DF69A); - - File Access 05/02/2006 12:45:53 net.exe C\WINDOWS\system32\net.exe

- ~5-feb-06 12:46:23~: el atacante cambia las entradas del registry que permiten el acceso remoto al sistema (En particular, HKLM\SYSTEM\CurrentControlSet\Terminal Server\fDenyTSConenctions =0) con Terminal Remoto: "REG ADD 'HKLM\System\CurrentControlSet\Control\Terminal Server' /v fDenyTSConnections /t REG_DWORD /d 0 /f

  + HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server tiene fecha de modificacion exactamente 12:46:23

  + File Access 05/02/2006 12:46:23 C\WINDOWS\system32\reg.exe

  + Security Event Log 05/02/2006 12:46:23 New Process Has Been Created -- New Process ID - 3984; Image

  + File Name - C:\WINDOWS\system32\reg.exe; Creator Process ID Domain - 3376; Username - Johnatan; Domain - COUNTERS; Logon ID - (0x0,0x3DF69A);

- ~5-feb-06 12:46:54 a 12:47:21~: El atacante ('ver0k') se conecta por Terminal Remoto al sistema desde la IP 70.107.249.155, distinta de la anterior.

  + Sec Event Log: 05/02/2006 12:47:21 Successful Logon - Username - ver0k; Domain - COUNTERS; Longo ID - (0x0,0x3F4E19); Method - ; Logon Process - User32 ; Authentication Package - Negotiate; Workstation - COUNTERS; - -;

  + Sec Event Log 05/02/2006 14:00:10 Session disconnected from
    winstation -- Username - ver0k; Domain - COUNTERS; Logon ID -
    (0x0,0x3F4E19); Mode - RDP-Tcp#1; Client Username - LUFERFU;
    Workstation - 70.107.249.155;

\newpage

** Línea temporal

De forma grafica y esquematica, senalando solo los eventos importantes,
nos queda pues el siguiente diagrama temporal que también es accesible
a través del siguiente [[./timeline/index.html][enlace:]]

[[./poc_timeline1.png]]

[[./poc_timeline2.png]]

[[./poc_timeline3.png]]

[[./poc_timeline4.png]]

[[./poc_timeline5.png]]

[[./poc_timeline6.png]]

[[./poc_timeline7.png]]

\newpage

** Conclusiones

Las siguientes conclusiones pueden ser extraidas de la investigacion de
este incidente.

- Conclusion 1 :: De forma global, a partir de los datos disponibles el
                  incidente se puede resumir en los siguientes hechos:

  + El sistema atacado es un Windows 2003 Server SP1, con licencia de
    evaluacion de 14 dias, de nombre COUNTERS.

  + Dicho sistema fue instalado y conectado a la red el 25 de enero
    de 2006.

  + El 26 de enero se instalaron en el sistema algunas aplicaciones,
    destacando entre ellas el sistema ERP de codigo abierto WebERP que a
    su vez emplea el servidor web Apache y la base de datos MySQL.

  + Desde dicha fecha hasta el 5 de febrero, el sistema mantuvo una

actividad que puede considerarse como normal, incluyendo algunos intentos de ataque al servidor web sin mayores consecuencias, la instalacion de alguna nueva aplicacion como PostGreSQL, y la copia de multiples ficheros de Microsoft Word, Powerpoint, Excel, documentos PDF e imagenes pornograficas en formato JPEG por parte de algun usuario.

+ El 5 de febrero, un atacante logro acceso con privilegios de administracion al sistema. Para ello, empleo metodos de ingenieria social, enviando un correo a un usuario del sistema con privilegios de administrador (Johnatan) a su cuenta en yahoo.com, incitandole a acceder con su navegador a una URL en la que el atacante tenia preparada un exploit.

+ Dicho exploit consistia en aprovechar una vulnerabilidad recientemente descubierta en la libreria GDI (Graphics Device Interface) existente en varias versiones de Windows, y entre ellas 2003 server (ver boletin de Microsoft en http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx); esta libreria se emplea para la generacion y presentacion de graficos en el sistema, y el exploit se ejecuto al acceder a un fichero grafico Windows Metafile (WMF) que no era tal sino que en realidad cargo un codigo (payload) que abrio una linea de comando al atacante sin que el usuario victima del engano se diera cuenta.

+ A continuacion, y una vez lograda una ventana como administrador, de forma inmediata el atacante procedio a crear una cuenta de nombre 'ver0k', dotandola de privilegios de administracion, y a modificar el sistema para permitir el acceso remoto al mismo.

+ El atacante accedió al sistema utilizando el servicio de Terminal Server.

+ Posteriormente el atacante procedio a buscar y visualizar los diferentes ficheros existentes bajo C:\Documents and Settings, incluyendo imagenes en formato JPEG, algun video, y con especial atencion archivos en formato .DOC. No pudo visualizar ficheros Excel, aunque lo intento, por cuanto esta aplicacion no estaba instalada en el sistema. Ficheros en otros formatos (Powerpoint o PDF) no fueron accedidos.

- Conclusion 2 :: El ataque al sistema se realizo con una cierta planificacion y con caracter especifico hacia este sistema en particular. Esta conclusion esta basada en los siguientes datos:

+ El correo enviado al usuario Johnatan a su cuenta para conseguir su colaboracion indirecta esta escrito en castellano, asi como simula

ser un contacto habitual del mismo (Alberto Lopez, Director General de Electronica y Computacion S.A.). Ademas, es en un segundo correo cuando se produce la intrusion real.

+ Una vez conseguido el acceso, y creado un usuario para su uso posterior, el atacante analiza muchos de los documentos existentes en el servidor.

- Conclusion 3 :: El ataque fue posible a pesar de que el sistema estaba, en general, bastante bien configurado y a un alto nivel de parcheo. Aunque es cierto que se utilizo una vulnerabilidad de reciente descubrimiento, fue el uso indebido del servidor para navegar de forma generica por Internet, especialmente grave cuando el usuario empleado para ello tiene privilegios de administracion, lo que posibilito el ataque.

- Conclusion 4 :: El analisis del sistema ha podido ser muy detallado gracias a que el administrador del mismo se preocupo de configurar en un alto nivel de detalle el sistema de auditoria de Windows, lo que demuestra la importancia de estar preparado por anticipado ante un posible ataque.

- Conclusion 5 :: En general, da la impresion de que el sistema no era un sistema en produccion real, sino un servidor preparado para generar una imagen que fuera posible usar en un reto de analisis forense. Esta conclusion esta basada en los siguientes datos:

+ El sistema esta instalado y en marcha con una licencia de evaluacion de Windows 2003 Server, unicamente valida para 14 dias.

+ En el sistema estan creados 16 cuentas de usuarios (ademas del administrador y la que crea el atacante) de las cuales unicamente se han empleado 4.

+ En el servidor se copiaron una gran cantidad de ficheros de Microsoft Excel, PowerPoint y Adobe PDF; sin embargo, ninguna de estas aplicaciones esta instalada. Aunque podria pensarse que los ficheros podrian ser accedidos desde la red, no fue asi en realidad tal y como revelan las fechas de creacion y acceso.

+ La primera reaccion de los administradores ante la creacion final de las cuentas del atacante en webERP y en el sistema, es intentar generar de forma inmediata una imagen del sistema, mas que analizar exactamente que estaba ocurriendo, o detener/desconectar de la red el sistema para minimizar el dano.

  + Algunas de las cuentas de correo de 'clientes' almacenadas dentro
    del sistema WebERP corresponden a dominios actualmente inexistentes
    en la realidad.

- Conclusion 6 :: Preservar la evidencia es crucial para cualquier
                  investigacion forense.

  En incidentes informaticos, como en incidentes de la vida real, la
  preservacion de la evidencia juega un papel fundamental en el proceso
  para asegurar el exito de la investigacion. En este incidente, mucha
  de la informacion ha sido posible obtenerla porque se disponia de una
  imagen binaria de la particion primaria del sistema en un instante de
  tiempo cercano al incidente y sin demasiadas modificaciones inducidas
  por el propio administrador del sistema. Si el administrador, cuando
  entro en el sistema para generar las copias, hubiera empezado a lanzar
  comandos para 'investigar', muchas de las pruebas habrian
  desaparecido. No modificar en absoluto la evidencia no es posible en
  la mayoria de los casos, pero siempre se debe intentar que la
  modificacion sea la menor posible.

\newpage

** Recomendaciones

Solucion al incidente

Como consecuencia del ataque, el sistema y la informacion en el
contenida han quedado completamente comprometidas. Aunque se ha
identificado el origen de la intrusion y algunas de la actividad
realizadas, no podemos estar absolutamente seguros de que no haya otros
cambios que han pasado desapercibidos a la investigacion forense. Por
tanto, para recuperarse de la intrusion y conseguir un sistema
completamente seguro los pasos recomendables serian, si ello es posible:

- Reinstalar una version limpia del sistema operativo, siempre sin estar
  conectado al exterior.

- Deshabilitar los servicios innecesarios.

- Instalar todos los hotfixes de seguridad.

- Consultar periodicamente las alertas de seguridad en este sistema
  operativo.

- Recuperar con cuidado datos de usuario de los backups y verificar los
  permisos (propietario, etc) de esos ficheros para que solo los
  usuarios que lo necesiten puedan acceder a ellos.

- Cambiar todos los passwords y, solo entonces, volver a conectarlo a la

red externa.

Una guia detallada de como recuperar un sistema de una intrusion puede encontrarse bajo:
http://www.cert.org/tech_tips/win-UNIX-system_compromise.html o en
http://www.nohack.net/recovery.htm

Alternativamente, como forma mas rapida, si bien carente del 100% de fiabilidad, la recuperacion de esta intrusion pasaria por, con el sistema desconectado de Internet:

- Eliminacion de las cuentas creadas por el atacante.

- Cambiar todos los passwords tanto del sistema como de la aplicacion webERP, y asegurar que dichos passwords cumplen unos estandares minimos de seguridad.

- Instalacion de los hotfixes de seguridad, especialmente los aplicables a la vulnerabilidad empleada en este ataque.

- Poner passwords para el acceso a MySQL Administrator.

Finalmente, el dano producido por la perdida de confidencialidad en la informacion (usuarios y clientes de la base de datos) debe mitigarse mediante las acciones de comunicacion, modificacion y/o legales que los responsables de la empresa consideren oportuno teniendo en cuenta su situacion comercial y los requerimientos legales que apliquen.

Recomendaciones finales

De cara a evitar posibles problemas similares a este en el futuro, se recomiendan las siguientes acciones:

- Instalar de forma inmediata los hotfixes de seguridad de Microsoft, a ser posible de forma automatica a traves de Windows Update.

- Asegurar que se minimiza el numero de cuentas con privilegios de administracion existentes, siendo recomendable dejar solo aquellas estrictamente necesarias.

- Instaurar una politica que asegure que no se emplean servidores en produccion para actividades personales como navegar por Internet, consultar el correo o jugar.

- Instalar algun sistema antivirus y antispyware, actualmente inexistente.

- Instalar algun programa de deteccion de intrusion y/o modificacion de ficheros clave del sistema operativo.

- Formar a los usuarios en la importancia de la seguridad y la
  existencia de ataques de 'ingenieria social' ante los que deben estar
  preparados.

- Asegurar que todos los sistemas de administracion (por ejemplo, MySQL)
  tienen palabras de acceso adecuadas para restringir su acceso.

- Guardar de forma cifrada la informacion de caracter confidencial, para
  minimizar la posibilidad de robo de la misma.

Asegurar que existe en la organizacion un sistema de gestion operativa
de la seguridad, que permita la prevencion, deteccion y eficaz reaccion
a ataques, en particular debe existir un adecuado mecanismo de alerta.

\newpage

** Anejos

Direcciones IP implicadas

134.186.42.18	Posible intento de ataque al web Server, el 29 de Enero a las 18:01:43 segun access.log
132.248.124.144	Intento de ataque al web Server, el 30 de Enero, a las 18:28:34
84.18.17.15	Origen de escaneo de vulnerabilidades del web Server, el 4 de Febrero a las14:04:43
4.18.17.15	Origen de escaneo de vulnerabilidades Sat Feb 04 14:19:14.
70.107.249.150	Dirección IP asociada al atacante
70.107.249.155	Dirección IP asociada al atacante
192.168.100.144	Escaneo de vulnerabilidades del web Server con nikto.
192.168.5.32	Escaneo de vulnerabilidades del web Server con nikto.
192.168.5.5	La propia direccion IP del sistema atacado, obtenida de HKLM\System\ControlSet001\Services\{5269ADEB-9E6D-4673-B898-4238F085972C}\Parameters\Tcpip\IPAddress, tambien dentro de esa misma subred privada.

Descripción de los méritos, menciones, titulaciones y certificaciones
experiencia y trayectoria que acreditan al investigador forense como
experto en la materia sobre la que se ha realizado el informe.

~José Luis Jerez~

~Gerente de Operaciones de Seguridad del SOC/CERT~

Soy el responsable de la coordinación del equipo del Centro de Operaciones de Seguridad (SOC) de Madrid y asesoro a los equipos de seguridad de los distintos centros internacionales para el alineamiento de los procesos de seguridad y resolución de problemáticas tecnológicas. Nuestro objetivo es facilitar a nuestros clientes servicios expertos, basados en procesos, de seguridad gestionada, complementados con servicios especializados como test de intrusión, homologación de seguridad en entornos de Juego On-line o análisis forense, garantizando los niveles de servicio establecidos (SLA).

Adicionalmente soy el responsable a nivel internacional del diseño, despliegue y puesta en marcha de proyectos de SOCs llave en mano, basado en una metodología propia cuyo desarrollo se ha basado en los años de experiencia prestando servicios expertos de seguridad y operación del SOC y las mejores prácticas de ITIL, ISO 20000, ISO 27000 y CERT/CC.

~Publicaciones~

PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS: Guía para la elaboración de Planes de Seguridad del Operador y Planes de Protección Específica.

Guía para la elaboración de Planes de Seguridad del Operador y Planes de Protección Específica, una ayuda técnica para los proveedores de seguridad en infraestructuras críticas (IICC).

La elaboración del documento surgió a raíz de la participación de la AEI Seguridad en el Grupo Informal de Protección de Infraestructuras Críticas (GIPIC), creado por el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC) del Ministerio del Interior. La Agrupación consideró interesante ampliar la información orientativa a aquellas empresas, fundamentalmente las PYME, motivadas en conocer qué se espera de los proveedores a la hora de implantar los instrumentos previstos por la estrategia española para la protección de dichas infraestructuras.

Así, la guía contribuye a una necesidad de mercado impulsada por la aprobación de la Ley que establece las medidas para la protección de las infraestructuras críticas y su desarrollo reglamentario que fija, entre otras, la necesidad de que los operadores críticos elaboren dos documentos:

Un Plan de Seguridad del Operador (PSO)

Un Plan de Protección Específico (PPE) para cada una de las infraestructuras que haya sido identificada como crítica por el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC)

Debido a que las guías oficiales sólo recogen los contenidos mínimos que deben articular estos planes, la AEI ha desarrollado este nuevo documento en el que se describe el modo de abordar la implantación de las medidas y más tarde reflejarlo en dichos Planes.

La Guía cuenta con dos grandes apartados alineados con la estructura del Plan de Seguridad del Operador (PSO) y del Plan de Protección Específico (PPE):

Un capítulo dedicado al análisis de riesgos, uno de los aspectos principales de los mencionados planes.

Dos capítulos dedicados a recoger las medidas de seguridad lógicas y físicas que se deberán implantar en las infraestructuras críticas para mejorar los niveles de protección integrales.

~Cursos~

- CHFI, Computer Hacking Forensic Investigation

- Imperva - SecureSphere Web Application Firewall and SecureSphere File Security & Compliance

- Imperva - SecureSphere Database Security and Compliance

- Palo Alto Networks Firewall 2.0

- Competencias y Habilidades Directivas

- Process Mining: Data science in Action

~Certificaciones~

- (ISC)2
  + CISSP, Certified Information System Security Professional
  + Licencia Certificate/ID number 380030

- ISACA
  + CISM, Certified Information Security Manager
  + Licencia Certificate/ID number 0708123

- ISACA
  + CISA, Certified Information Systems Auditor

```
  + Licencia Certificate/ID number 0651861

- AlienVault
  + OCSA: OSSIM Security Analyst
  + AlienVault

- AlienVault
  + OCSE: OSSIM Security Engineer
  + AlienVault

- RSA, The Security Division of EMC
  + CSE: RSA enVision Certified Systems Engineer
  + The Security Division of EMC

- ISACA
  + CRISC, Certified in Risk and Information Systems Control
  + Licencia Certificate/ID number 1108411

- Sourcefire
  + SFCP, Sourcefire Certified Professional

- Sourcefire
  + SFCSE, Sourcefire Certified Security Engineer

- Sourcefire
  + SFCSR, Sourcefire Certified Sales Rep

~Educación~

- Universidad Politécnica de Madrid
  + Facultad de Informatica
```

Documento de aceptación de fin de proyecto

Una vez finalizado el proyecto se firma un documento en el que se acepta su adecuada finalización por ambas partes implicadas.
El técnico investigador deberá de guardar una copia en un lugar seguro en previsión de que sea llamado a testificar en el largo plazo.

```
#+TITLE: DOCUMENTACIÓN DE ACEPTACIÓN DE FIN DE PROYECTO
#+AUTHOR:   José Luis Jerez Guerrero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+OPTIONS:  H:3 num:nil toc:nil \n:nil @:t ::t |:t ^:t -:t f:t *:t
#+OPTIONS: TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+OPTIONS: author:nil date:nil tags:nil todo:nil
#+TAGS: Actual (a) Pendiente(p) Finalizado (f)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
```

Código del Proyecto: {{{codProy}}}
Fecha: {{{date(%d-%m-%Y)}}}

{{{nomCli}}}, en representación de {{{empCli}}}, confirma la correcta finalización del servicio de {{{tipoServ}}}, realizado en cumplimiento del contrato firmado entre las partes.

D./Dª {{{nomCli}}}
Firma

Capítulo 9: CONCLUSIONES Y LÍNEAS FUTURAS

Conclusiones

Tras finalizar el proyecto, la primera **conclusión** personal, evidente e inmediata es que no hay como dedicar tiempo a alguna materia con suficiente interés para llegar a tener un nivel de conocimiento importante de la misma.
Cuando empecé el PFC, a pesar de tener ya alguna experiencia profesional acerca de lo que todo el mundo llama análisis forense, era consciente de que mis conocimientos eran muy rudimentarios, sobretodo por la gran cantidad de dudas que tenía acerca de los pasos a seguir, las acciones a realizar o no realizar y en general acerca de todo el proceso.
Tras investigar acerca de todo el proceso de investigación informática forense he llegado a la **conclusión** de que incluso realizando la mejor de las investigaciones forenses, incluso sin cometer errores y desarrollando los informes con claridad, es posible que no sea suficiente para que sea adecuadamente utilizado en un proceso judicial, ya que existe un factor no controlado dentro del mismo, que es la propia condición humana y el nivel de conocimiento de la persona que debe de juzgar los resultados presentados.
Sin embargo, y a pesar de lo comentado en el apartado anterior, la principal **conclusión** que he sacado es que cualquier investigación informática forense debe de ser llevada a cabo por personal cualificado tanto técnicamente como a nivel normativo y legal. Además, la investigación debe de ser extremadamente metodológica, basarse en buenas prácticas y ser documentada exhaustivamente, hasta el punto de disponer de la metodología utilizada de forma previa al inicio de la investigación para evitar la necesidad de requerir 'ideas felices' que pueden poner en riesgo la integridad de la investigación.
Dado que se ha **concluido** la necesidad de disponer de una metodología explícita, coherente y documentada adecuadamente, la siguiente **conclusión** inmediata es que Emacs, tras una importante curva de aprendizaje, es claramente una alternativa que cumple con cualquier requisito relativo al uso de un procesador de textos que pueda requerir una investigación informática forense, por más compleja que sea la misma. Además, su capacidad para funcionar en cualquier plataforma de uso común, su facilidad para integrarse con otras herramientas y su versatilidad a la hora de gestionar tareas y tiempos, la posibilidad de trabajar con ficheros cifrados desde el momento inicial del proyecto y sobretodo su integración con distintos lenguajes muy potentes de programación y la posibilidad de desarrollar la documentación siguiendo los paradigmas de la programación literaria, derivan en la clara **conclusión** de que Emacs es la herramienta clave para el eficiente desarrollo de la investigación desde el punto de vista de la gestión y seguridad de la misma.
Finalmente, en relación al objetivo de limitar el uso de herramientas forenses a aquellas que pueden ser utilizadas e integradas directamente por Emacs, la **conclusión** clara está en el mismo planteamiento, el uso exclusivo de herramientas forenses que pueden ser utilizadas e integradas directamente en Emacs es una limitación en si mismo, y por lo tanto un error de procedimiento.

Líneas futuras

Derivado de las anteriores concusiones y del conocimiento adquirido tangencialmente durante la investigación creo que hay un gran potencial en la idea de base planteada, pero debe de ser correctamente replanteado. Existen más iniciativas como DFF (Digital Forensics Framework) por ejemplo, con objetivos similares pero con distinto acercamiento, aunque igualmente acertado.
Obviamente, el mayor cambio a realizar, es eliminar la limitación del uso exclusivo de herramientas forenses que pueden ser utilizadas e integradas directamente por Emac, si bien éstas deben de ser maximizadas por motivos obvios, a igualdad de resultados frente a otras herramientas sobretodo con interfaces gráficas.
En relación a la metodología planteada, dado que he seguido las buenas prácticas internacionales actuales, soy consciente de que en el futuro próximo estas van a ser ampliadas y con toda seguridad mejoradas,

por lo que habrá que mantener alineada la metodología propuesta con las buenas prácticas que se publiquen.
Además, sería muy interesante desarrollar un `laboratorio forense` en el que se dispusiese de distintos equipos, cada uno de ellos con un sistema operativo distinto y sus correspondientes herramientas e investigar la viabilidad de disponer de un equipo principal con acceso por ssh a los anteriores para centralizar desde éste la investigación.
Por otro lado, en la actualidad proliferan los sistemas distribuidos o `cloud computing platforms`, y creo que este proyecto podría integrarse en nuevos planteamientos que tratan de dar solución a investigaciones realizadas en dichas plataformas como Digital Forensic Tools for the OpenStack Cloud Computing Platform, desde un punto de vista metodológico y de integración.
Igualmente, otro de los campos donde podría investigarse su adecuada integración es en el nuevo campo de moda, el llamado `Big data`, sobretodo teniendo en cuenta que sleuthkit dispone de un framework orientado a utilizar Hadoop para procesar imágenes de disco.
Finalmente, en relación con la documentación y la evolución de la programación literaria, sería interesante tratar de alinear el actual planteamiento con la documentación reactiva.

Capítulo 10: GLOSARIO

El glosario no se ha desarrollado de forma explícita ya que he utilizado la capacidad de org-mode de enlazar fácilmente los conceptos con URLs en los que se da su correspondiente descripción en tiempo real.
Creo que es más útil dedicarle tiempo a un glosario dinámico, independiente del contenido estático que pueda expresar en el proyecto, y asociar la explicación de los conceptos a entidades donde su descripción es más amplia y su posibilidad de actualización es mayor.
Sin embargo, en caso de identificar conceptos o siglas que considere que son interesantes para dejarlos reflejados estáticamente en este proyecto, aparecen a continuación.

Capítulo 11: BIBLIOGRAFÍA

Bibliografía

- http://es.wikipedia.org
  - http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico
  - http://es.wikipedia.org/wiki/C%C3%B3mputo_forense
  - http://es.wikipedia.org/wiki/Criminalística
  - http://es.wikipedia.org/wiki/C%C3%B3mputo_forense
  - http://es.wikipedia.org/wiki/M%C3%A9todo_cient%C3%ADfico
- http://www.elladodelmal.com/2012/04/analisis-forense-de-metadatos-15.html
- http://seguinfo.wordpress.com/category/analisis-forense/
- http://luisvilanova.es/
  - http://luisvilanova.es/peritos-informaticos-analsis-forense/
  - http://luisvilanova.es/norma-une1970012011-base-para-las-periciales-informaticas/
- http://conexioninversa.blogspot.com.es/
  - http://conexioninversa.blogspot.com.es/2008/11/te-gusta-el-anlisis-forense-ponte.html
- http://www.slideshare.net/slideshow/embed_code/17377044#
- http://www.youtube.com/watch?feature=player_embedded&v=JDaicPIgn9U
- http://www.antpji.com/index.php/ique-es-un-perito-informatico
- http://www.thingsupsecurity.com/
- http://noticias.juridicas.com/base_datos/Penal/lecr.l2t5.html
- http://noticias.juridicas.com/base_datos/Privado/r41-l1-2000.html
- http://conexioninversa.blogspot.com.es/2013/12/artefactos-forenses-i.html
- http://conexioninversa.blogspot.com.es/2014/01/artefactos-forenses-ii-prefetch-y.html
- http://insecuredata.blogspot.com.es/2015/03/artefactos-forenses-i.html
- http://insecuredata.blogspot.com.es/2015/03/artefactos-forenses-ii.html
- http://orgmode.org
  - http://orgmode.org/manual/Working-With-Source-Code.html#Working-With-Source-Code
  - http://orgmode.org/manual/Literal-examples.html#Literal-examples
    - http://orgmode.org/worg/org-contrib/babel/intro.html
    - http://orgmode.org/worg/org-contrib/babel/how-to-use-Org-Babel-for-R.html
- http://www.literateprogramming.com/index.html
- https://github.com/limist/literate-programming-examples
- http://vasc.ri.cmu.edu/old_help/Programming/Literate/literate.html

Metodología

- http://es.wikiquote.org/wiki/Sherlock_Holmes
- http://www.cienciaforense.com/Pages/es/computers/comp.html
- Importance of a standard methodology in computer forensics
- http://cp4df.sourceforge.net/index.html
- http://www.seinhe.com/blog/87-el-proceso-de-analisis-forense-informatico
- http://policiasenlared.blogspot.com.es/2011/11/la-cadena-de-custodia-informatico.html
- http://www.elderecho.com/www-elderecho-com/contaminacion-custodia-invalida-periciales-inform11_556555001.html#nota1
- http://en.wikipedia.org/wiki/Electronic_discovery
- http://www.kelvintopset.com/resources/how-to-write-the-investigation-report
- http://insecurityit.blogspot.com.es/2013/09/reflexiones-sobre-la-norma-isoiec.html
- http://www.portaley.com/delitos-informaticos/
- http://www.oas.org/juridico/spanish/cyb_analisis_foren.pdf
- http://peritoit.com/2013/12/08/utilizacion-de-un-programa-espia-para-el-despido-por-uso-ind
- http://peritoit.com/2012/06/03/rfc-3227directrices-para-la-recopilacion-de-evidencias/
- http://www.egarante.com/validez-legal-de-egarante/
- http://www.sidertia.com/media/6fcbe47e-e7dc-4967-af14-22e828fa112e/-673106981/Documentos/Un%20forense%20llevado%20a%20juicio_1.0_SDT.pdf

Documentación

- Acuerdo de confidencialidad

Emacs/Orgmode/LaTeX

- http://stackoverflow.com/questions/15255080/how-to-auto-close-an-auto-encryption-mode-buffe
- http://stackoverflow.com/questions/7246212/elisp-create-unnamed-buffer-from-contents-of-file
- http://emacs-fu.blogspot.com.es/2011/04/nice-looking-pdfs-with-org-mode-and.html
- http://nickguthrie.com/archives/276
- http://juanreyero.com/article/emacs/org-teams.html
- http://www.gigamonkeys.com/book/

- http://sachachua.com
  - http://pages.sachachua.com/emacs-notes/how-to-read-emacs-lisp

  +http://sachachua.com/blog/wp-content/uploads/2013/05/How-to-Learn-Emacs8.png
- http://www.masteringemacs.org/articles/2011/02/08/mastering-key-bindings-emacs/
- http://www.gnu.org/software/emacs/manual/html_node/elisp/index.html#Top
- http://www.gnu.org/software/emacs/manual/html_node/emacs/index.html#Top
- http://www.blackhats.es/wordpress/
- http://www.dotemacs.de/basics.html
- http://www.rpublica.net/emacs/
- http://orgmode.org/manual/index.html#Top
- http://www.emacswiki.org/emacs/VictorPeinado
- http://www.emacswiki.org/emacs/AutoEncryption
- http://www.emacswiki.org/emacs/ElispCookbook
- http://www.emacswiki.org/emacs/InteractiveFunction
- http://tex.stackexchange.com/questions/76105/what-does-restricted-write18-enabled-mean-

Vídeos

- http://hangouton.es/video-peritaje-informatico-herramientas-y-cadena-de-custodia/

Herramientas

- Listado de artefactos.
  - http://conexioninversa.blogspot.com.es/2013/12/artefactos-forenses-i.html
  - http://conexioninversa.blogspot.com.es/2014/01/artefactos-forenses-ii-prefetch-y.html
  - http://insecuredata.blogspot.com.es/2015/03/artefactos-forenses-i.html
  - http://insecuredata.blogspot.com.es/2015/03/artefactos-forenses-ii.html
- Listado de aplicaciones.
  - https://santoku-linux.com/ : Mobile forensics
  - http://resources.infosecinstitute.com/registry-forensics-regripper-command-line-li
  - http://resources.infosecinstitute.com/windows-registry-analysis-regripper-hands-ca
  - https://www.elhacker.net/InfoForenseWindows.html
- Timeline
  - http://blog.templatemonster.com/demos/build-a-vertical-timeline-archives-page-usin

Capítulo 12: ANEXOS

Documentación anexa en la carpeta DOC_ANEXA

```
bash-3.2$ pwd
/Users/error0x01/pfc
bash-3.2$ cd DOC_ANEXA/
bash-3.2$ ls
ISO_IEC_27037_2012.pdf
UNE_197001_2011.pdf
org-info.js
pfc.el
regripper_plugins.csv
regripper_plugins.pdf
worg.css
bash-3.2$
```

ISO_IEC_27037_2012.pdf Documento estándar facilitado por AENOR.

UNE_197001_2011.pdf Documento estándar facilitado por AENOR.

org-info.js Javascript utilizado para generar la documentación en HTML.

pfc.el Fichero emacs-lisp con la funcionalidad desarrollada.

regripper_plugins.csv Listado en formato csv de los plugins de Regripper.

regripper_plugins.pdf Listado en formato pdf de los plugins de Regripper.

worg.css CSS utilizado para generar la documentación en HTML.

Emacs: Conocimientos mínimos para enfrentar un análisis forense

Es cierto que la curva de aprendizaje de Emacs no es precisamente ágil, y que los inicios pueden ser un poco complicados. Sin embargo, todo lo que merece la pena tiene un coste, y en este caso se trata de dedicarle tiempo y ser constante.
Para facilitar el proceso de aprendizaje, a continuación se describen los conocimientos y los comandos comúnmente más utilizados:

Convenciones

Para seguir adecuadamente el presente capítulo se tiene que tener presente las siguientes convenciones:

- `C` se hace referencia a `Ctrl`.
    - `C-c` equivale a pulsar simultáneamente Ctrl y la tecla 'c'.
- `M` se hace referencia a `Alt` (o *Meta*).
    - `M-c` equivale a pulsar simultáneamente Alt y la tecla 'c'.
    - En teclados Apple, con la tecla *Apple*.
- `S` se hace referencia a `SHIFT`.
    - `S-c` equivale a pulsar simultáneamente Shift y la tecla 'c'.

- Otras convenciones son:
    - Las cadenas a introducir como el `comando`, `nombre de archivo` o `cadenas de búsqueda` se representarán en `código`.
    - `C-h k` equivale a pulsar simultáneamente Ctrl y la tecla 'h' y posteriormente la tecla 'k'.
    - En general, el nombre de una tecla encerrado entre <>indicará la acción de pulsar dicha tecla. Representación de teclas:
        - <Enter>Enter.
        - <Space>Espacio.
        - <Back>Retroceso.
        - <Tab>Tabulación.
        - <Shift>Mayúsculas.
        - <Bizqdo>Botón izquierdo del ratón.
        - <Bdrcho>Botón derecho del ratón.
        - <Bcentro>Botón central del ratón.

Emacs dispone de varias formas para la ejecución de los distintos comandos. A continuación se van a enumerar las distintas posibilidades disponibles junto a un ejemplo común. Este ejemplo permitirá saber, en cada caso, la forma de ejecutar una búsqueda de una secuencia concreta y el reemplaza por una segunda:

- Nombre de comando: Para ejecutar un comando hay que pulsar `M-x` y `nombre de comando`.
    - Por ejemplo, `M-x replace-string`.
- Mediante la pulsación de una determinada secuencia de teclas, específica para cada comando.
    - Por ejemplo, pulsar `M-%`.
- Mediante las opciones de menú.
    - Por ejemplo, en la siguiente imagen podemos ver la opción de menú para el reemplazo de una secuencia.

En este manual se explicarán los comandos más útiles a la hora de desarrollar un análisis forense, y su ejecución mediante la pulsación de la secuencia de teclas correspondiente, que denominaremos comando. Quizás pueda parecer, disponiendo de la posibilidad de realizar las operaciones mediante las opciones del menú de Emacs, que el ejercicio de memoria que supone la ejecución de comandos mediante la pulsación de una determinada secuencia de teclas, puede implicar una complicación innecesaria. Sin embargo, a medida que se conoce más acerca de la utilización de Emacs, se aprecian las ventajas que supone sobre todo en el uso de los comandos de utilización más frecuente, en factores tan importantes como la productividad, y eficiencia.
Finalmente, comentar que la combinación de teclas que Emacs asocia a cada comando es una combinación que presenta por defecto. La instalación y customización de Emacs (secuencias de teclas incluidas) no es objeto de este PFC, y se encuentra ampliamente documentado, por lo que el usuario puede modificar la misma y adaptarla a su gusto.

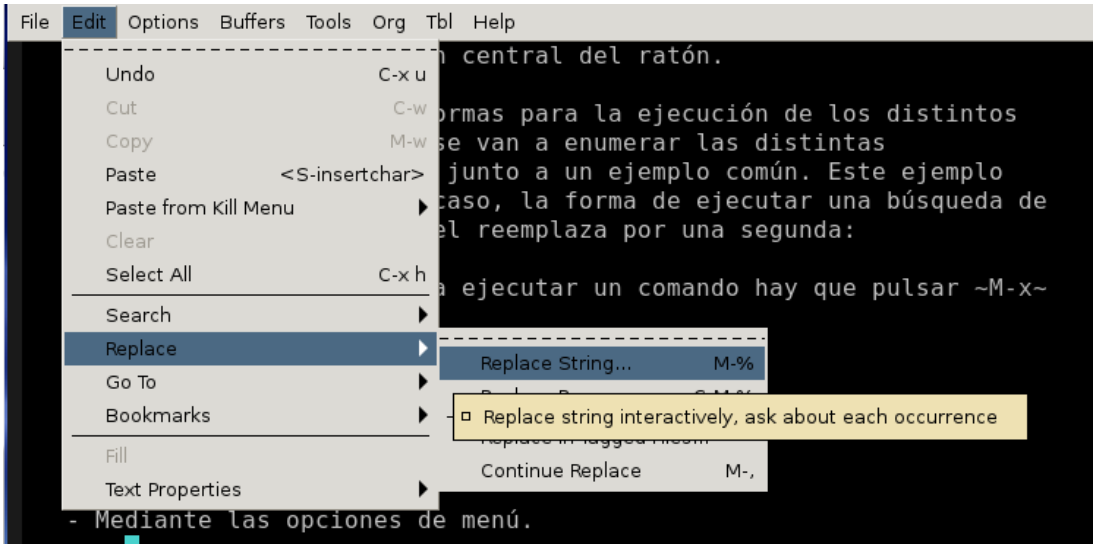


Figura 1: Ejemplo de reemplazo en emacs

Ayuda de Emacs

La ayuda de Emacs es muy amplia, pero con los siguientes comandos se resuelven un tanto por ciento muy amplio de las necesidades de un neófito en Emacs:

- `C-h t` Lanza el tutorial de Emacs (’Learn by doing’).
- `C-h k SECUENCIA_DE_TECLAS` Ayuda para conocer la funcionalidad de las secuencias de teclas.
- `C-h v VARIABLE` Consulta el uso y valor de las variables del entorno Emacs.
- `C-h a PATRÓN` Hace *apropos* de las funciones, es decir busca un listado de funciones según una cadena o parte de ella dada.
- `C-h f FUNCION` Muestra la documentación de la función nombrada.
- `C-h F COMANDO` Muestra la documentación del comando nombrado.

Configuración inicial

- Buffers

  Existe un concepto fundamental cuando hablamos de edición de texto, los archivos de texto. Emacs `no edita` archivos. Cuando Emacs se ’encuentra’ (usando terminología Emacs), un archivo original, independientemente de su localización física, éste es copiado en un buffer temporal, donde se realiza toda la actividad de edición.

  Igualmente, cuando creamos una ventana de texto en Emacs, lo que hacemos es crear un buffer. Emacs lo gestiona todo mediante buffers, hasta que el usuario decide ’salvar’ el contenido, momento en el que se almacena el contenido del buffer en un archivo.

  Los buffers tienen un nombre, y normalmente, éste suele coincidir con el de su archivo asociado. Sin embargo, existen buffers que no tienen archivos asociados, cuyo nombre normalmente empieza y termina con el carácter *. El ejemplo más evidente es el buffer **scratch**, de gran utilidad, ya que es el equivalente al `scratch paper`.

  Los comandos que facilitan el trabajo con los buffers son:

- `C-x C-b` Lista de buffers.
- `C-x C-s` Guardar el contenido de un buffer en un archivo.
- `C-x C-right/left` Acceder al siguiente/posterior buffer.
- `C-z` Comando para salir de Emacs temporalmente, para que pueda regresar a la misma sesión de Emacs después escribiendo 'exit'.

- Modos

  Emacs dispone de modos de edición mayores y menores, que es como conseguimos que Emacs se adecue a la tarea concreta a desarrollar.

  Por ejemplo, Emacs dispone, entre otros, de *modo texto* para la redacción, *mode Marckup* para lenguajes como LaTeX, HTML, SGML o XML, *modos de programación* para distintos lenguajes (Python, Lisp, Java, Perl, etc), un *modo mail*, para el correo correo....etc. Si bien, es posible desarrollar modos ad-hoc, personalizados para distintas necesidades particulares.

  Al seleccionar un modo, el entorno de Emacs 'transforma' el editor de forma que se adecuado al tipo de tarea que estemos realizando en cada momento.

  Cada buffer debe tener un y solo un modo mayor activado en cada momento. Alguno de los modos mayores que más nos pueden interesar son:

  - `fundamental-mode`: Modo por defecto.
  - `org-mode`: Para editar utilizando ORG-MODE, orientado a GTD.
  - `Emacs-Lisp`: Para programar en eLisp.
  - `shell-mode`: Para utilizar una shell desde Emacs.
  - `text-mode`: Para edición de texto.
  - `view-mode`: Para el visionado de archivos (no edición).
  - `elisp-mode`: Escribir programas en Lisp.
  - `perl-mode, sgml-mode, html-mode`: Para programar en cada uno de los distintos lenguajes.

  Los modos menores definen aspectos concretos del entorno de Emacs. Algunos de los modos menores más comúnmente utilizados son:

  - `isearch-mode`: Para búsquedas.
  - `auto-encription-mode`: Para cifrado.
  - `overwrite-mode`: Sobrescribe en lugar de insertar.
  - `abbrev-mode`: Permite la utilización de abreviaturas.
  - `auto-save-mode`:Guarda automáticamente en un archivo especial.
  - `paragraph-indent-text-mode`: Sangra la primera línea de cada párrafo.

  En este caso, hay un solo comando para interactuar con los modos:

  - `M-x nombre de modo` Activa los modos, ya sean mayores o menores, y desactiva los modos menores activos.

  Estos cambios son visibles, como se verá en el apartado siguiente, en la `'línea de modo'` o 'mode line'.

- Configuración

  Para personalizar o adaptar Emacs a nuestras necesidades particulares hay que realizar cambios en los parámetros que Emacs nos presenta por defecto. Estos cambios requieren, en algunos casos, desde un simple clic hasta conocimientos de programación en Lisp.

  Las alternativas para modificar la configuración de Emacs son:

  - Utilizando el comando `M-x custom`.
  - Pulsando sobre el icono de la barra de herramientas que representa una hoja y un lápiz escribiendo.
  - Mediante las opciones de menú `Options`.
  - Editando directamente el archivo de configuración `.emacs`.

  En los tres primeros casos, al acceder a `Custom`, se presenta una pantalla por la que podemos utilizar el ratón o las teclas habituales en Emacs. Al inicio aparecen las siguientes opciones que afectan a todo el buffer:

  - *Set for Current Session*: Para guardar los cambios de modo que afecten sólo a la presente sesión de Emacs.
  - *Save for Future Sessions*: Los cambios que serán guardados en el archivo de configuración `.emacs`, de manera que seguirán vigentes en futuras sesiones.
  - *Reset*: Deshace los últimos cambios realizados, asumiendo los valores anteriores a dichos cambios.
  - *Reset to Saved*: Deshace los últimos cambios realizados con `Save for Future Sessions`, asumiendo los valores anteriores a dichos cambios.
  - *Erase Custonization*: Deshace todo cambio realizado por `Custom`, tanto si se ha realizado realizado a través de `Set for Current Session` como a través de `Save for Future Sessions`.
  - *Finish*: Cierra el presente buffer, pasando a la pantalla anterior.

  Cuando iniciamos Emacs, se intenta cargar un programa Lisp desde un archivo de inicialización. Emacs busca su archivo de inicio utilizando los nombres de fichero `~/.emacs`, `~/emacs.el` o `~/.emacs.d/init.el`. Puede optar por utilizar cualquiera de estos tres nombres.

  Para alguien que no va a hacer un uso extensivo de Emacs y con conocimientos básicos, en mi opinión, debería de basar su configuración en el fichero `~/.emacs`.

  Un ejemplo [1] muy generalista es el que se muestra a continuación. Sin embargo, dotemacs.de dispone de muchos ejemplos prácticos para aquellos que desean profundizar en el tema.

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;                  Mi fichero .emacs
;;   (Retazos tomados prestados de diferentes lugares)
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;


;; --- Modos iniciales y por defecto ---

;; Mi info personal
```

[1] Basado en `http://www.emacswiki.org/emacs/VictorPeinado`

```
(setq user-full-name 'José L Jerez')

;; Mi situación geográfica
(setq calendar-latitude 40.20)
(setq calendar-longitude -3.52)
(setq calendar-location-name 'Móstoles, Madrid')

;; No quiero barra de scroll
(scroll-bar-mode -1)

;; Ni barra del menú
(menu-bar-mode nil)

;; Muestra la batería del portatil
(display-battery)

;; Usa avisos visuales, no sonoros.
(setq visible-bell 1)

;; La tecla 'Supr' borra la parte seleccionada
(pending-delete-mode 1)

;; No muestres los mensajes de inicio, ya los conozco
(setq inhibit-startup-message t)

;; No muestres claves en el buffer
(add-hook 'comint-mode-hook
          (lambda ()
            (add-to-list 'comint-output-filter-functions
                         'comint-watch-for-password-prompt)))

;; Usa y/n en lugar de yes/no
(fset 'yes-or-no-p 'y-or-n-p)

;; Usa como fuente por defecto
(set-face-font 'default 'lucidasanstypewriter-14')

;; Mis ficheros elisp están en
(setq my-lisp-directory (expand-file-name '=/emacs-lisp/'))

;; Carga el directorio de los ficheros elisp
(add-to-list 'load-path my-lisp-directory)

;; Modo inicial texto
(setq vc-initial-comment 't)
(setq default-major-mode 'text-mode)
(setq initial-major-mode 'text-mode)
(add-hook 'text-mode-hook
          (function (lambda ()
```

```
                    (turn-on-auto-fill))))

;; Colores por defecto
(set-foreground-color 'grey100' )
(set-background-color '#000044' )

(set-cursor-color 'yellow')
(set-border-color 'DarkSlateGray' )

;; No crees ficheros temporales xxx=
(setq make-backup-files nil)

;; Remarca la zona seleccionada
(transient-mark-mode +1)

;; Abre archivos comprimidos con gzip y bzip2
(auto-compression-mode 1)

;; Muestra el número de línea y de columna
(line-number-mode 't)
(column-number-mode 't)
(require 'icomplete)

;; Habilita las tildes y demás
(standard-display-european +1)
(set-input-mode (car (current-input-mode))
                (nth 1 (current-input-mode))
                0)
(set-language-environment 'Latin-1')

;; Usa el corrector ispell en español
(defun ispell-check ()
  (interactive)
  (if mark-active
      (if (< (mark) (point))
  (ispell-region (mark) (point))
(ispell-region (point) (mark)))
    (ispell-buffer)))

;; Para utilizar aspell, quita el comentario de la línea siguiente
;; (setq ispell-program-name 'aspell'')
(setq ispell-local-dictionary 'castellano8')

;; Algunas combinaciones de teclas útiles
(global-set-key '\C-g' 'goto-line)
(global-set-key '\M-i' 'indented-text-mode)
(global-set-key '\C-c\c' 'compile)
(global-set-key [?\M-\C-q] 'fill-region)
```

```
;; --- Teclas de función personalizadas ---

;; F6: arranca la shell con el modo eshell
(global-set-key [f6] 'eshell)

;; F7: cambia el diccionario por defecto
(global-set-key [f7] 'ispell-change-dictionary)

;; F8: comprueba una palabra con ispell
(global-set-key [f8] 'ispell-word)

;; F9: comprueba el buffer actual con ispell
(global-set-key [f9] 'ispell-check)

;; F10: arranca el calendario
(global-set-key [f10] 'calendar)


;; --- Calendario y diario ---

;; Archivo del diario
(if (file-exists-p '=/docs/diario')
    (setq diary-file '=/docs/diario'))

;; Calendario europeo y nombres en español
(setq calendar-week-start-day 1
      european-calendar-style t
      calendar-day-name-array
      ['Domingo' 'Lunes' 'Martes' 'Miércoles'
       'Jueves' 'Viernes' 'Sabado']
      calendar-month-name-array
      ['Enero' 'Febrero' 'Marzo' 'Abril' 'Mayo'
       'Junio' 'Julio' 'Agosto' 'Septiembre'
       'Octubre'' 'Noviembre' 'Diciembre'])

(setq view-diary-entries-initially t
      mark-diary-entries-in-calendar t
      number-of-diary-entries 7)
(add-hook 'diary-display-hook 'fancy-diary-display)
(add-hook 'today-visible-calendar-hook 'calendar-mark-today)

;; --- fin de .emacs ---
```

Como puede verse a lo largo de todo el fichero de ejemplo, cada comando del archivo .emacs se corresponde con una función Lisp, que tiene la estructura `(nombre_de_la_funcion argumentos)`, como `(scroll-bar-mode -1)`, donde *-1* aparece como argumento de la función.

Por otro lado, en el desarrollo del ejemplo se puede ver que aparecen los argumentos `t`, que equivale a verdadero o activado y `nil`, equivalente a falso o desactivado, como por ejemplo `(setq`

`make-backup-files nil)`, empleado para deshabilitar los archivos de copia de seguridad.

La edición del archivo `.emacs` puede hacerse desde el propio Emacs, mediante el comando `C-x C-f` y, tras seleccionar el mismo, el archivo de configuración se presentará en un nuevo buffer en el que puede modificarse normalmente. Además, el archivo `.emacs` no es imprescindible para el funcionamiento del editor, por lo que en cualquier momento puede borrarse y crear otro.

- Mode line

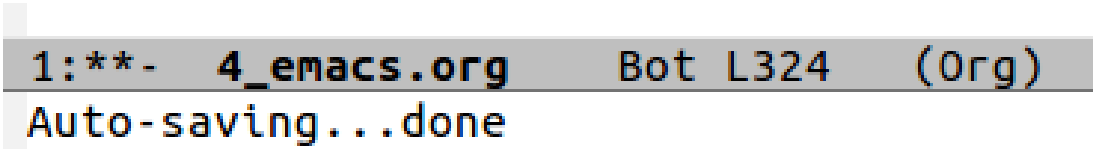


Figura 2: Línea de modo

En general, la pantalla de Emacs, ya sea en un terminal o en modo gráfico, es bastante sencilla y muy intuitiva. Sin embargo, la barra inferior o línea de modo]] es poco intuitiva.

Los elementos que componen la línea de modo, de izquierda a derecha, según la imagen anterior:

- El primer parámetro es la codificación de los caracteres. En particular '1' implica el uso de *iso-latin-1-unix* y 'U' se corresponde con el juego de caracteres *utf-8-unix*.
- Tras la identificación del juego de caracteres y los ':' el:
  - Si el primer carácter aparece como:
    - **%** si el buffer es de sólo lectura. Es el más interesante, ya que pulsando sobre el mismo (o mediante `C-x C-q`) permite configurar el comportamiento del buffer como de lectura o lectura/escritura.
    - **-** si el buffer es de lectura/escritura y no ha sido modificado o se han salvado las últimas modificaciones.
    - **/*** si el contenido del buffer ha sido modificado, y no se han salvado estas modificaciones.
  - Si el segundo carácter hace referencia , utilizando el mismo tipo de simbología, al estado de modificación del buffer.
  - El tercer carácter presenta el path del directorio raíz donde buscará los documentos.
- Nombre del buffer.
- Porción visible del contenido del buffer (en %). En el caso de que se vea todo el contenido del buffer, aparecerá `All \=Todo`. En este caso aparece `Bot`, ya que el cursor se encuentra al final del contenido del buffer.
- Número de la linea en que se encuentra el cursor.
- Modo Mayor. En este caso es `Org`.
- Modo Menor activo. En este caso no se ha activado ninguno.

Para una mejor comprensión del modo de línea se recomienda utilizar el siguiente código:

```
;; use setq-default to set it for /all/ modes
(setq mode-line-format
  (list
    ;; the buffer name; the file name as a tool tip
```

```
'(:eval (propertize '%b ' 'face 'font-lock-keyword-face
    'help-echo (buffer-file-name)))

;; line and column
'(' ;; '%02' to set to 2 chars at least; prevents flickering
  (propertize '%02l' 'face 'font-lock-type-face) ','
  (propertize '%02c' 'face 'font-lock-type-face)
') '

;; relative position, size of file
'['
(propertize '%p' 'face 'font-lock-constant-face) ;; % above top
'/'
(propertize '%I' 'face 'font-lock-constant-face) ;; size
'] '

;; the current major mode for the buffer.
'['

'(:eval (propertize '%m' 'face 'font-lock-string-face
          'help-echo buffer-file-coding-system))
'] '


'[' ;; insert vs overwrite mode, input-method in a tooltip
'(:eval (propertize (if overwrite-mode 'Ovr' 'Ins')
          'face 'font-lock-preprocessor-face
          'help-echo (concat 'Buffer is in '
                      (if overwrite-mode 'overwrite' 'insert') ' mode')))

;; was this buffer modified since the last save?
'(:eval (when (buffer-modified-p)
          (concat ','  (propertize 'Mod'
                        'face 'font-lock-warning-face
                        'help-echo 'Buffer has been modified'))))

;; is this buffer read-only?
'(:eval (when buffer-read-only
          (concat ','  (propertize 'RO'
                        'face 'font-lock-type-face
                        'help-echo 'Buffer is read-only'))))
'] '

;; add the time, with the date and the emacs uptime in the tooltip
'(:eval (propertize (format-time-string '%H:%M')
          'help-echo
          (concat (format-time-string '%c; ')
                  (emacs-uptime 'Uptime:%hh'))))
' __'
```

```
;; i don't want to see minor-modes; but if you want, uncomment this:
;; minor-mode-alist  ;; list of minor modes
'%-' ;; fill with '-'
))
```

Aplicando estos cambios, la línea de modo aparecerá con el formato de la imagen que se ve a continuación:

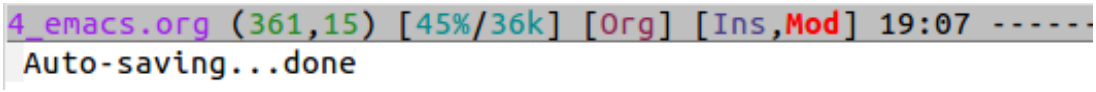


Figura 3: Línea de modo adaptada

Bajo la línea de modo se encuentra el 'mini-buffer'. En esta franja de la pantalla aparecen las salidas de los comandos tecleados, mensajes de Emacs y, entre otras cosas, es el lugar donde se especifican las búsquedas o los comandos específicos a efectuar.

- ORG-MODE

  El modo Org (*Org-mode*), es un modo de edición del editor de texto Emacs mediante el cual se editan documentos jerárquicos en texto plano. Su uso encaja con distintas necesidades, como la creación de notas de cosas por hacer, la planificación de proyectos y hasta la programación de distintos lenguajes. Es por este cúmulo de capacidades por las que he seleccionado Emacs como editor ya que desde la versión 22, el modo Org es parte de su distribución oficial de Emacs, aunque también dispone de entregas separadas, con lo que las versiones más recientes del modo Org con respecto a la que se incluye en Emacs también están disponibles.

  El modo Org permite, por ejemplo, gestionar elementos 'to-do' (cosas por hacer), pueden disponer de prioridades, propiedades y fechas de arranque o vencimiento; pueden estar subdivididos en subtareas o en listas de verificación, así como generarse automáticamente una agenda de las entradas de cosas por hacer.

  La mayor parte del comportamiento del modo Org puede personalizarse mediante los procedimientos habituales en Emacs, tal y como se ha visto anteriormente.

  El manual de Org-mode es la referencia más completa a la que se puede acceder para conocer todo lo necesario acerca del modo Org. Sin embargo, a continuación describo una serie de conceptos y comandos, de Emacs y Org-mode, que considero necesarios para acometer un proyecto de análisis forense basado en Emacs.

Comandos básicos

Una vez ejecutado Emacs, en mi experiencia, los comandos básicos más utilizados son:

- `C-x b` Acceder a un buffer existente (seleccionando del listado que aparece) o crear un nuevo buffer (escribiendo el nombre del mismo) no asociado a ningún fichero existente.
- `C-x C-f` Abrir un fichero existente (seleccionando un fichero del sistema de ficheros) o crear uno nuevo (accediendo a un directorio y escribiendo un nombre nuevo para un fichero).
- `C-x C-c` Cerrar Emacs.
- `C-g` Para detener un comando que esté tomando mucho tiempo para ejecutarse y para descartar un argumento numérico o el comienzo de un comando que no quiere finalizar.

Figura 4: Logo Org-mode

- `C-x u` Comando deshacer.
- `C-v` Avanzar una pantalla completa.
- `M-v` Retroceder una pantalla completa.

Ventanas

La pantalla es el espacio que proporciona el editor para escribir. Sin embargo, se puede subdividir en varias ventanas, lo que permite visualiza paralelamente varios archivos distintos. Uno en cada ventana. Algunos de los comandos que permiten la gestión de las ventanas y el desplazamiento por las mismas son:

- `C-x 1` Expande la ventana que contiene el cursor, para ocupar toda la pantalla. Esto borra todas las demás ventanas.

- C-x 2 Divide la pantalla en dos ventanas horizontales.
- C-x 3 Divide la pantalla en dos ventanas verticales.
- C-x o Mover el cursor a otra ventana.

Copiar, cortar, insertar y borrar

Quizás este sea uno de los puntos más autoexplicativos del proyecto, sin embargo, puede verse que no tiene nada que ver con el típico C-c, C-v y C-x 'de toda la vida'.
En el caso de Emacs, los comandos más comunes de un editor se corresponden con:

- C-<Space> Inicia la selección de texto (marca) que hay que realizar con los cursores.
- C-x C-x Intercambia marca y cursor.
- M-h Selecciona el párrafo actual.
- C-x h Selecciona todo el buffer.
- M-w Comando para COPIAR.
- C-w Comando para CORTAR.
- C-y Comando para PEGAR. Reinserta el último texto copiado, cortado o eliminado, en la posición actual del cursor.
- La diferencia entre 'eliminar' y 'borrar' es que el texto 'eliminado' puede ser reinsertado ('yanking' o 'pegar') mientras que el texto 'borrado' no puede ser reinsertado.
- C-u /número n/ /simbolo/ Inserta n veces el símbolo.
- <Delback> Borra el carácter justo antes que el cursor.
- M-<Delback> Elimina la palabra inmediatamente antes del cursor.
- C-d Borra el siguiente carácter después del cursor.
- M-d Elimina la siguiente palabra después del cursor.
- M-k Elimina hasta el final de la oración actual.
- C-k Elimina desde el cursor hasta el fin de la línea.

Buscar y reemplazar

En la línea del apartado anterior, a continuación se describen los comandos]] más utilizados para la localización y modificación de texto:

- C-s Para búsqueda hacia adelante y teclee C-s de nuevo, para buscar la siguiente ocurrencia.
- C-r Búsqueda hacia atrás.
- M-% Buscar y reemplazar (uno a uno).
- C-c \/ Permite realizar búsquedas en elementos dispersos del documento en función de expresiones regulares, fechas o incluso propiedades. Son los árboles dispersos o *sparse trees*.

Es posible complementar las búsquedas más clásicas con las búsquedas globales en el árbol, que te permite encontrar resultados globales en el documento.

Formato de texto

- Los diferentes formatos para enfatizar el texto que es posible utilizar en Emacs son:

  - **bold**
  - *italic*
  - underlined
  - `code`
  - `verbatim`
  - ~~strike-through~~

  que se codifican de tal como puede verse en el siguiente ejemplo:

```
*bold*
/italic/
_underlined_
~code~
=verbatim=
+strike-through+
```

- Para insertar un salto de línea: Se utiliza * \ *
- Comentario Los comentarios nunca se exportan. Se utiliza #

  - Otra forma es utilizar

```
#+BEGIN_COMMENT
Este texto no ser  exportado y no ser  exportado
#+END_COMMENT
```

- Párrafo

```
#+BEGIN_VERSE
Great clouds overhead
Tiny black birds rise and fall
Snow covers Emacs

     -- AlexSchroeder
#+END_VERSE
```

> Great clouds overhead
> Tiny black birds rise and fall
> Snow covers Emacs
>
> – AlexSchroeder

- Cita

```
#+BEGIN_QUOTE
Everything should be made as simple as possible,
but not any simpler -- Albert Einstein
#+END_QUOTE
```

> Everything should be made as simple as possible, but not any simpler – Albert Einstein

- Texto centrado

```
#+BEGIN_CENTER
Everything should be made as simple as possible, \\
but not any simpler
#+END_CENTER
```

Everything should be made as simple as possible,
but not any simpler

Tablas

Las tablas son elementos fundamentales a la hora de presentar datos en cualquier proyecto. En el caso de Org-mode, se tratan en ASCII plano.

- Las tablas se crean:
  - Mediante 'l' o *pipe*, utilizado como separador de columna.
  - Utilizando `C-c |` y especificando el número de filas por columnas (Ej. 5x2).
- Se accede mediante <TAB>a los diferentes campos.
- `C-c C-c` redimensiona los campos sin mover el cursor.
- Se ponen las divisiones horizontales de columnas mediante `C-c -` o `C-c <INTRO>`.
- Para desplazar una columna se utiliza `M-<-` o `M-->`.
- El ancho de la columna es determinado por el editor de tablas. Para limitar el ancho de una columna debemos tener un campo llamando *<N>* donde **N** es el ancho máximo de caracteres por columna. Las columnas que sean mas anchas se acortaran y añadirán **=>** indicando que hay mas texto, que podrá ser editado mediante `C-c '`.
- Ejemplo de tabla:

Esto es una tabla	otra celda
hola hola	hola
444	€€

- A partir de las tablas es posible realizar cálculos mediante fórmulas o comandos concretos. Para ello, lo que podemos utilizar son los siguientes comandos:
  - `C-c }` Se numeran o identifican las filas mediante , lo que permite pensar en las fórmulas a aplicar con mayor facilidad.

    - `C-c *` Calcula fila actual.
    - `C-u C-c *` Calcula todas las filas.
    - `C-c +` Suma los números de la columna actual, de un rectángulo definido o bien de una región activa, el resultado es mostrado en *minibuffer* y puede ser insertado con `C-y`.

- No es parte del objetivo de este proyecto conocer en detalle el manejo de Emacs como hoja de cálculo. Sin embargo, si el lector tiene interés en profundizar sobre este aspecto, el manual de Org-mode explica todo lo necesario, como que para asignar una formula a un campo en particular, debe ir precedido por *:=*, o que las fórmulas son guardadas en el formato especial con `#+TBLFM:` directamente debajo de la tabla. Además debemos usar el comando C-u C-c = si queremos insertar una nueva formula en el campo actual.

A continuación se muestra un ejemplo de una tabla en la que se calcula el importe multiplicando la cantidad y el precio, y en la décima fila, quinta columna, se calcula el sumatorio de los importes.

Item	Und	Cant	Precio	Importe
Asado	Kg	2.0	40	80.00
Vacío	Kg	1.5	40	60.00
Chori	Kg	2.0	20	40.00
Pollo	Kg	2.0	35	70.00
Pan	Kg	1.5	15	22.50
Carbón	Kg	9.0	20	180.00
Fernet	Lt	3.0	50	150.00
Coca	Lt	9.0	8	72.00
				674.50

```
#+TBLFM: $5=$3*$4;%0.2f@10$5=vsum(@I..@II);%0.2f
```

Listas

Las listas planas permiten estructurar una información dentro de un documento. Las listas pueden ser desordenadas u ordenadas, y las descripciones siempre se desarrollan tras el símbolo ”.
Las *líneas de cabecera*, también llamadas *títulos* (de diferente nivel) o `headline` empiezan con una estrella (’*’) si son de primer nivel, los de segundo nivel con dos estrellas (’**’), y así sucesivamente. Cada uno de estos niveles de títulos se asocia a un concepto similar a los capítulos o subcapítulos de un documento, y Emacs permite navegar ente ellos de forma ágil.
Con el objetivo de poder realizarlo de forma ágil y eficiente a continuación se facilitan una serie de keystrokes relacionados con headlines simples:

- `<Tabulador>` (sobre un headline) Permite visualizar el contenido del mismo u ocultarlo.
- `M ->` (sobre un headline) Evoluciona el nivel de headline a un subnivel.
- `M <-` (sobre un headline) Evoluciona el headline actual a un nivel superior.
- `M-S <Enter>` Para insertar una nueva tarea.
- `S ->` Cambia el bullet entre una serie de opciones (-,+,*).

Tareas

Crear listados de tareas o TODOs es una actividad muy común a la hora de abordar un proyecto.
Es importante tener en cuenta que los ítems *TODO* o tareas por realizar son siempre headlines. Sin embargo, un headline no tiene porque estar asociado a una tarea.
Una tarea a realizar se establece asignando a un headline la palabra *TODO*:

```
* TODO headline 1 asociado a una tarea
** Headline de segundo nivel no asociada a una tarea
** TODO Tarea de segundo nivel
*** TODO Subtarea de la segunda tarea
```

Con el objetivo de poder realizarlo de forma ágil y eficiente a continuación se facilitan una serie de keystrokes relacionados con headlines asociados a tareas:

- `S <-` o `S <-` Selecciona el estado siguiente o anterior de `TODO`.
- `C-c t <letra>` Saltara directamente a estado asociado a la letra. Si la letra es el <Espacio>, se eliminara cualquier clave `TODO` de la lista.

Cuando trabajamos con tareas, es importante gestionar adecuadamente los `estados` que componen la secuencia de la misma.
Los estados se pueden establecer:

- Directamente sobre el fichero de configuración de Emacs.

```
(setq org-todo-keywords
 '((sequence 'TODO(t)' '|' 'DONE(d)')
   (sequence 'REPORT(r)' 'BUG(b)' 'KNOWNCAUSE(k)' '|' 'FIXED(f)')
   (sequence '|' 'CANCELED(c)')))
```

- A nivel de fichero individual.

```
#+TODO: TODO | DONE
#+TODO: REPORT BUG KNOWNCAUSE | FIXED
#+TODO: | CANCELED
```

Además de los estados, una tarea se puede priorizar. Org permite tres prioridades (A, B y C) siendo A la máxima prioridad. Las prioridades se reflejan solo en la agenda, fuera de ella no tienen efecto.

- `C-c ,\` Asigna la prioridad a la tarea actual (A, B o C). Si se pulsa SPC la prioridad es eliminada.
- `S Flechas arriba/abajo` : Asigna prioridades de forma circular [#A][#B][#C]

Para modificar las prioridades de una tarea de un buffer individual se puede hacer mediante: `#+PRIORITIES: Alta Media Baja`.
Otra forma de mostrar las tareas es mediante *checkboxes*:

- Para crear los checkbox se escribe '-' y `C-u C-c C-c` para que aparezca '[ ]' y para activar/desactivar pulsamos `C-c C-c`.
- Para ir generando una lista pulsamos `M+Intro` al finalizar cada item.
- Para indentar una lista pulsamos `M+Flechas_horizontales`.

- Para mover las tareas y subtareas en vertical pulsamos `M+Flechas_verticales`.
- Si ponemos *[0%]* a la altura de una lista calcula el % de tareas completadas al pulsar `C-c C-c`.
- Si ponemos *[0/0]* a la altura de una lista calcula el numero de tareas completadas al pulsar `C-c C-c`.
- Ejemplo: [0%] [0/1]
  - ⊟ tarea 1
    - ☒ subtarea 1
    - ☐ subtarea 2

Marcas

Una forma de relacionar información, de varios temas distintos, dispersa por el documento, es usar TAGS (marcas o etiquetas) en las lineas de cabecera. Cada linea de cabecera puede contener una lista de TAGS. Para usar los TAGS definidos en un solo fichero podemos usar una lista:

```
#+TAGS: @Jose @Fran
#+TAGS: @Reun(r) @DOCS(d) @PROY(p) @Datos(d)
#+TAGS: @_CRITICO_

* Proyecto Forense H486      :PROY:
** DONE Reunión con el cliene    :Jose:Reun:
** DONE Firma de documentos      :Fran:DOCS:_CRITICO_:
** TODO Toma de datos             :Jose:Datos:
```

Los keystrokes más utilizados para trabajar con TAGS son:

- En el caso de que el listado de TAGS sea dinámico se deja la lista de `#+TAGS:` en blanco.
- `C-c C-c` Crea TAGS para la linea de cabecera actual.
- `C-c \` Busca la siguiente aparición del TAG que se especifique.
- Existen TAGS especiales, como 'noexport', que permiten comportamientos particulares. En este caso, todos los headlines con 'noexport' asociado no serán exportados en el caso de que el documento.

Propiedades

En primera instancia se puede pensar que trabajar con propiedades o columnas no aporta ningún tipo de ventaja a la hora de desarrollar un proceso forense. La organización es un aspecto muy importante dentro del proceso de trabajo, y el uso de propiedades (o *drawers*) o columnas permite optimizar aspectos concretos a nivel organizativo.
Para trabajar con las propiedades es un requisito entender como trabajar con tablas y listas en Org-mode. Las propiedades en Org-mode está formada por binomios ':nombre_propiedad:valor' que se definen y se pueden aplicar a nivel de headlines.
Los keystrokes básicos para el uso de las propiedades son:

- `C-c C-x p` Asigna un valor a una propiedad.

- `C-c C-c` Ejecuta comandos de la propiedad.
- `C-c C-c d` Elimina una propiedad de la entrada actual.
- `C-c \` Crea un árbol donde guarda todas las entradas que coincidan.

Un ejemplo de aplicación de propiedades a evidencias forenses podría ser el siguiente:

```
* Evidencias
** Archivo con contrase as
 :PROPERTIES: , :ID: FI-180 , :STATUS: FIRMADA , :ASSIGNED: jljerez
 :END:
** Imagen evidencia NTP
 :PROPERTIES:
  :ID:         IM-190
  :STATUS:     FIRMADA
  :ASSIGNED:   jljerez
  :END:
```

Las propiedades se pueden heredar desde los niveles superiores a los inferiores. Nombrando la propiedad como ':nombre_propiedad_ALL:valor1 valor2 valor3' es posible definir los valores permitidos (valor1, valor2, valor3) para una propiedad concreta ':nombre_propiedad:'.
A continuación se presenta un ejemplo de herencia y predefinición de valores para unas determinadas propiedades. En el primer nivel se establecen las propiedades a heredar (identificadas porque terminan en *_ALL*) y en niveles inferiores se utilizan los valores predefinidos.

```
* Evidencias
 :PROPERTIES:
 :STATUS_ALL:     FIRMADA NO_FIRMADA ANULADA PERDIDA
 :ASSIGNED_ALL: jljerez aperez flopez
 :END:
** Archivo con contrase as
 :PROPERTIES: , :ID: FI-180 , :STATUS: ANULADA , :ASSIGNED: jljerez
 :END:
** Imagen evidencia NTP
 :PROPERTIES:
  :ID:         IM-190
  :STATUS:     NO_FIRMADA
  :ASSIGNED:   flopez
  :END:
```

Las propiedades especiales permiten acceder de forma alternativa a estas funcionalidades, por ejemplo:

TODO Tarea TO-DO de la entrada.

TAGS TAGS definidos directamente en una linea de cabecera.

TIMESTAMP La primera fecha de una entrada.

DEADLINE El límite de tiempo.

SCHEDULED El tiempo o timestamp de esta entrada.

CLOSED Cuando fue realmente cerrada esta entrada.

CATEGORY La categoría de la entrada.

PRIORITY La prioridad de la entrada.

ITEM El contenido de una entrada.

Columnas

La `vista de columnas`, es una capa superpuesta u overlay sobre un buffer, ya que se trata de una vista y no de un modo, que permite identificar y modificar propiedades de las columnas. Cada headline será convertido en una fila tabulable, si bien es cierto que es posible definir el formato a distintos niveles según el punto en el que se defina *COLUMNS*.
Para aplicar el formato a nivel de fichero se añade una línea en la cabecera del mismo, si bien esta vista no es la más interesante a la hora de utilizarla en un proyecto. A continuación se presenta una definición básica que referencia a algunas de las propiedades especiales:

```
#+COLUMNS: %20ITEM %TIMESTAMP %TODO %TAGS %PRIORITY
```

Los keystrokes más útiles para trabajar con columnas son:

- `C-c C-x C-c` Activa la vista de columna, y con ésta activa, entre otros podemos utilizar:
  - `r` Recrea la vista de columna.
  - `q` Sale de la vista de columna.

Quizás la mayor utilidad de las columnas sea que, definiendo propiedades a nivel de headline y sus herederos, es posible formatearlas a conveniencia de cada uno.
De forma general, en el siguiente ejemplo podemos observar un modo de empleo de las capacidades mencionadas aplicadas en una parte de un proceso forense digital.

```
* Pruebas forenses realizadas
  :PROPERTIES:
  :COLUMNS: %25ITEM %9Pruebas(Pruebas?){X} %Equipo %11Estado %10Tiempo_Estimado{:}
  :Equipo_ALL: SRV1 SRV2 FW_FORTINET1 SW_CISCO_1 PC1 PC2
  :Estado_ALL: No iniciado En progreso Finalizado Cancelado
  :Pruebas_ALL: [ ] [X]
  :END:
```

El formato de la línea *:COLLUMS:* para dada una de las propiedades (*%Nomb_propiedad*) tiene la siguiente sintaxis:

```
%[ancho]propiedad[(titulo)][{tipo_sumario}]
```

Donde podemos añadir los siguientes atributos, algunos de los cuales se pueden ver reflejados en el ejemplo anterior:

- `ancho` un valor entero que indicara el ancho de la columna en caracteres.
- `propiedad` la propiedad a ser editada en esta columna.
- `(titulo)` La cabecera del texto para la columna.
- `{tipo_sumario}` Si se especifica, el valor de las columnas para el padre serán computadas para los hijos.
- `{+}` Suma los miembros en esta columna.
- `{$}` Divisas.

- `{:}` Suma los tiempos HH:MM:SS.
- `{X}` Estado del checkbox, [X] si todas los hijos son [X].
- `{X/}` Estado del checkbox, [n/m].
- `{X%}` Estado del checkbox [n%].
- `{min}` El numero más pequeño de la columna.
- `{max}` El mayor número de la columna.
- `{mean}` Significado aritmético de los valores.
- `{:min}` El valor de tiempo más pequeño de la columna.
- `{:max}` El mayor valor de tiempo de la columna.
- `{:mean}` Significado aritmético de los valores de tiempo.
- `{@min}` Edad mínima (en días/horas/minutos/segundos).
- `{@max}` Edad máxima (en días/horas/minutos/segundos).
- `{@mean}` Significado aritmético de los valores (en días/horas/minutos/segundos).

Otra utilidad a la hora de trabajar con la documentación en Emacs sería la posibilidad de utilizar esta vista como resumen o índice de la información que aporta. Sin embargo, la vista de columnas no puede ser exportada o impresa directamente, por lo que es necesario usar *bloques dinámicos de vistas de columnas*.

Los keystrokes básicos para gestionar bloques dinámicos son:

- `C-c C-x i` Inserta un bloque dinámico capturando una vista de columna.
- `C-c C-c` Actualiza el bloque dinámico actual, estando el cursor al principio de la linea de dicho bloque #+BEGIN.

La utilización de bloques dinámicos permite, tal como se puede ver a continuación, trabajar con vistas de columnas accediendo dinámicamente a los buffers activos:

ITEM	TODO	PRIORITY	TAGS
* ¿Por qué Emacs?	DONE		:Finalizado:
* Emacs: Conocimientos mínimos para enfrentar un análisis forense	WORK		:Actual:
** Convenciones	DONE		:Finalizado:
** Ayuda de Emacs	DONE		:Finalizado:
** Conceptos básicos y configuración inicial	DONE		:Finalizado:
** Comandos básicos	DONE		:Finalizado:
** Ventanas	DONE		:Finalizado:
** Copiar, cortar, insertar y borrar	DONE		:Finalizado:
** Buscar y reemplazar	DONE		:Finalizado:
** Formato de texto	DONE		:Finalizado:
** Tablas	DONE		:Finalizado:
** Listas	DONE		:Finalizado:
** Marcas	DONE		:Finalizado:
** Propiedades	WORK		:Finalizado:
** Columnas	WORK		:Actual:
** Links	WORK		:Pendiente:
** Gestión del tiempo	TODO		:Pendiente:
** Acceder a la agenda	TODO		:Pendiente:
** Añadir fechas	TODO		:Pendiente:
** Exportar a	TODO		:Pendiente:
** Trabajar con código fuente	TODO		:Pendiente:
** Extensiones de ORG	TODO		:Pendiente:
** Cifrado de información	TODO		:Pendiente:
** elisp: programación de pruebas	TODO		:Pendiente:
** Abrir archivo (Ej. M-x gtd)	TODO		:Pendiente:
** Emacs/LaTeX: presentación profesional	TODO		:Pendiente:

Los atributos que podemos utilizar para formatear la vista de columna con bloques dinámicos son:

- `:hlines` Cuando es t, inserta una linea horizontal después de cada linea. Cuando es un numero N, inserta una linea horizontal antes de cada linea de cabecera con un nivel inferior o igual a N.
- `:id` Es el identificador, que puede ser local, global, `ruta-al-fichero` o directamente el ID.
- `:maxlevel` Cuando tiene un valor N, no captura las entradas por debajo del nivel N.
- `:vlines` Cuando es t, fuerza los grupos de columnas para tener lineas verticales.
- `:skip-empty-rows` Cuando es t, ignora las filas donde no hay indicada una linea en blanco para un ITEM.

Enlaces

Los enlaces son una facilidad muy interesante a la hora de documentar, ya sean enlaces a otros apartados del mismo documento, a otros documentos que se encuentran en el mismo equipo o externos al mismo o a otro tipo de fuentes de información.
Generalizando se puede distinguir entre enlaces internos y externos al documento editado.
Los enlaces internos se establecen mediante dos elementos, 'objetivo' y 'enlace'.
El enlace más simple, que permite acceder a un headline directamente, se construye escribiendo entre dos corchetes el headline al que se desea acceder. Por ejemplo:

```
[[Comandos básicos]]
```

En los enlaces internos algo más evolucionados, el 'objetivo', se establece escribiendo una combinación de caracteres entre '' (por ejemplo, «OBJ_234») y el 'enlace' al mismo, que puede utilizarse a su vez de forma básica, esto es, cuando se desea crear un enlace y el nombre que se le quiere dar al mismo es idéntico al objetivo o si se desea que la descripción del enlace sea más descriptiva. En el siguiente ejemplo podemos ver ambos casos:

```
[[OBJ_234]] - Mismos caracteres para el objetivo y el enlace.
[[OBJ_234][Objetivo 234]] - Descripción del enlace distinta al objetivo.
```

En relación a enlaces externos, ya sea a archivos o a otro tipo de información, los tipos de enlaces más utilizados en un proyecto forense son los siguientes:

```
[[http://www.error0x01.net/]] Enlace a una URL de una web.

[[file:/home/usuario/fichero.txt]] Enlace a un archivo con PATH absoluto. Se puede
utilizar igualmente sin /file:/.

[[file:documentos/presentacion.pdf]] Enlace a un archivo con PATH relativo. Se puede
utilizar igualmente sin /file:/.

[[file:documentos/presentacion.pdf22]] Enlace a la línea 22 del
archivo /presentacion.pdf/.

[[file:tmp.orgtexto a buscar en un headline]] Busqueda de texto en el
headline del archivo tmp.org

[[file:/usuario@equipo_remoto:carpeta/archivo.pdf]] Enlace al
/archivo.pdf/ de la /carpeta/ del /equipo_remoto/ (ya sea nombre
de equipo o dirección IP) al que se desea acceder. Se puede
utilizar igualmente sin /file:/.

[[file+sys:/ruta/al/archivo/ejecutable]] Equivale a hacer doble click
sobre el archivo.

[[file+emacs:/ruta/al/archivo/]] Forzar que se habra con Emacs.

[[docview:/ruta/al/archivo/doc.pdf22]] Habre en doc-view mode en la
página 22.

[[mailto:jljerez@error0x01.net]] Enlace para crear un correo.

[[irc:/freenode.net/#emacs/over]] Enlace IRC.

[[shell:ls -la *.org][shell:ls -la *.org]] Enlace a un comando shell.

[[elisp:org-agenda]] Enlace a un comando interactivo Elisp.

[[elisp:(find-file-other-frame "elisp_forense.org")]] Enlace a un
formulario lisp a evaluar.
```

La sintaxis que permite crear los enlaces es muy similar a la de los enlaces internos ya comentada. La forma más básica de crear un enlace es cuando el enlace y el nombre que se le quiere dar al mismo es idéntico. En este caso se escribe el enlace entre dos corchetes tal como puede verse en el ejemplo de una URL:

```
[[http://www.error0x01.net/]]
```

Si se desea diferenciar entre el enlace y la descripción del mismo, se escribe entre corchetes el enlace, seguido de su descripción, cada una de ellas entre corchetes tal como se muestra a continuación:

```
[[file:/usuario@equipo:carpeta/archivo.pdf][Fichero remoto]]
```

Las combinaciones de teclas a utilizar para trabajar con enlaces son:

- `C-c C-l` Inicia el proceso de insertar un enlace. Pulsamos TAB para ver el tipo de enlace (Ej. mailto:, shell, bbdb, etc) y el objetivo del tipo adecuado, para finalizar añadiendo la descripción del mismo si se desea.
- `C-u C-c C-l` Insertar un enlace a un archivo.
- `C-c C-o` Acceder al enlace.

Finalmente, las notas a pie (footnotes) son un tipo concreto de enlace. En nuestro caso vamos a considerar dos tipos de *footnotes*.

```
[fn:autonumérica] y [Definición en línea en LaTeX]
```

Se trata de las notas a pie típicas. En el primer caso se crea un indicador, del tipo `[fn:1]`, a la altura del concepto tratado y se crea un headline al final del texto en el que aparece la misma notación seguida de su descripción.
`C-c C-x f` es el keystroke que crea una *footnote* en caso de que no exista, y si se encuentra de una definición, al pulsarlo se salta a la primera referencia del mismo.
La segunda construcción, al exportar a LaTeX el documento, y pulsar sobre la referencia, aparece la definición sobre la misma.
En ambos casos `C-C C-c` sobre una referencia implica salar a la definición de la misma.

Imágenes

Insertar una imagen es una tarea sencilla, muy similar a los enlaces ya que, en esencia, lo que se hace es una llamada a una imagen, del mismo modo que se realiza una llamada a un fichero o una RL.
En un contexto normal insertar una imagen se define con tres simples líneas. Un subtítulo, el identificador de la imagen y la ruta a la misma o utilizando :

```
#+CAPTION: Subtitulo de la imagen IMG-0101.
#+NAME:   fig:IMG-0101
[[./images/ejemplo.png]]

o podemos utilizar [[file:images/ejemplo.png]]
```

Gestión del tiempo

Este apartado es, quizás, uno de los más importantes de cara a la ejecución controlada de un proyecto, en este caso, de análisis forense digital.
Con el entorno de trabajo planteado, es posible usar fechas con distintos formatos e intervalos de tiempo para la planificación del proyecto.
Es particularmente interesante el uso de una agenda, que permite lleva una planificación a futuro así como realizar consultas a posteriori de las actividades realizadas. Además, permite optimizar la gestión de las tareas al introducir la posibilidad de realizar cálculos de tiempos empleados en tareas concretas que se pueden automatizar más adelante total o parcialmente, en función de su uso.

- Marcas de tiempo

  Para gestionar el tiempo, el elemento principal es el que permite el registro del mismo. En este caso, utilizaremos *marcas de tiempo* o *timestamps*.

  Las marcas de tiempo se pueden utilizar con distintos objetivos según su formato. Algunos de los usos más extendidos son:

  - Indicar eventos globales que no tienen impacto en la planificación, o dicho de otro modo, son marcas inactivas como *[2014-02-23 dom]*.
  - Asociar eventos globales a la agenda con el fin de planificar una tarea. Son marcas activas como *<2014-02-23 dom>*.
  - Es posible concretar, en los dos casos descritos, la hora concreta con la que se relaciona el evento, ya sea activo *<2014-02-23 dom 11:56>* o no *[2014-02-23 dom 11:56]*.
  - Los intervalos de tiempo son otro tipo interesante de marca de tiempo, que permite asociar tareas y su esfuerzo en tiempo. Como se verá más adelante, esta capacidad tiene múltiples utilidades en el planteamiento de un proyecto, sea cual fuere, ya que permite planificar a futuro, cuantificar el esfuerzo estimado, y finalmente, medir el esfuerzo real realizado. Un ejemplo del formato utilizado es *[2014-02-23 dom 12:00 - 12:45]* para intervalos diarios, o *<2014-02-20 jue>* - *<2014-02-23 dom>*.
  - Es posible definir eventos que se deben de repetir en el tiempo para concretar acciones reiterativas cíclicamente, con un intervalo de N días (d), semanas (w), meses (m), o años (y). El formato para identificar este tipo de acciones es *<2014-02-23 dom 1 d>*, lo que programaría diariamente la tarea asociada.

  Los keystrokes más utilizados para trabajar con marcas de tiempo son:

  - `C-c !` Inserta una `fecha inactiva` que no aparece en la agenda y timeline.
  - `C-c .` Inserta una `fecha activa` que aparece en la agenda y timeline.
  - `C-u C-c !` / `C-u C-c .` Insertan una `fecha inactiva / activa` en la que aparece reflejada la hora.
  - `C-c C-s` Establece una propiedad '*SCHEDULED*' o fecha programada de inicio para un determinado headline asociado a una tarea.

```
*** Empezar el proyecto
SCHEDULED: <2012-11-15 jue>
```

  - `C-c C-d` Establece una propiedad '*DEADLINE*' o fecha límite para un determinado headline asociado a una tarea que debe de terminar. Es posible configurar una fecha límite periódica añadiendo '*+1m*', para establecer deadlines mensuales.

```
*** Terminar el proyecto
DEADLINE: <2014-06-06 vie>
```

- Se pueden combinar ambos para poner una fecha de inicio y otra de fin, e incluso que se repita una acción TODO, que al pasar a DONE se actualiza la fecha.
- `C-c C-c` Al pulsar sobre el una fecha se normaliza la misma, y se verifica si el formato y datos son correctos.
- `S-<flechas>` Al pulsarse sobre una fecha, hace avanzar o retroceder la misma en el calendario u horario.

- Trabajando con tiempos

  Un proyecto tiene una fecha de inicio y una fecha de fin. Dentro de dicho intervalo temporal se van a desarrollar una serie de actividades y tareas de tiempo indeterminado, pero que normalmente debe de ser estimado a prori. Posteriormente, o en tiempo real, si se dispone de la información adecuada, es posible identificar desviaciones o situaciones no controladas, así como las mejoras en la eficiencia de los procesos.

  En ese aspecto, Org-mode es una herramienta precisa y potente, que permite, a un usuario con los conocimientos suficientes, optimizar sus procesos y disponer de medidas para ello.

  En el apartado anterior se ha visto el manejo de marcas de tiempo, que es el concepto básico. A continuación se verán prácticas más avanzadas que permiten trabajar con tiempos.

  Org-mode dispone de un reloj que puede arrancarse cuando comience una tarea y se inicia una tarea y pararlo tras finalizarla, o tomar intervalos de tiempos y posteriormente analizaros. De esa forma podemos estimar el tiempo y esfuerzo realizado. Es particularmente interesante ya que permite hacerlo entre distintas sesiones de emacs, de tal manera que no importa cuantas veces hayamos parado e iniciado dicho reloj. Para ello hay que introducir las siguientes lineas en nuestro .emacs:

  ```
  (setq org-clock-persist 'history)
  (org-clock-persistence-insinuate)
  ```

  Los keystrokes que permiten trabajar con el reloj son los siguientes:

  - `C-c C-x C-i` : Inicia el reloj actual, insertando la palabra CLOCK junto al timestamp. Las lineas de tiempo van asociadas a una propiedad (o drawer) denominada *:LOGBOOK:*.

  ```
  * Registar tiempos de una tarea o item.................2:26
  ,   :LOGBOOK:
     CLOCK:[2012-02-14 mar 00:45]--[2012-02-14 mar 01:58]=>1:13
     CLOCK:[2012-02-13 lun 00:45]--[2012-02-13 lun 01:58]=>1:13
    ,  :END:
  ```

  - `C-c C-x C-o` : Detiene el contador de un reloj añadiendo un timestamp frente a la tarea detenida.
  - `C-c C-x C-e` :Actualiza el esfuerzo estimado para la tarea actual.
  - `C-u C-c C-x C-i` : Selecciona una tarea de una lista de tareas cronometradas.
  - `C-c C-c` ó `C-c C-y` : Vuelve a calcular el intervalo de tiempo después de cambiar uno de los timestamps.
  - `C-c C-t` : Cambia el estado de una tarea, por lo que el reloj en caso de existir para dicha tarea se detendrá.

- `C-c C-x C-x` : Cancela el reloj actual. Es útil cuando se inicia el reloj por error para alguna tarea.
- `C-c C-x C-j` : Salta al headline de la tarea usada en el reloj actual. Útil para identificar la tarea en la que se está registrando el tiempo.
- `C-c C-x C-d` : Muestra el sumario de tiempos para cada subárbol del buffer actual.

Como se ha comentado anteriormente, Org-mode puede facilitar información bastante compleja basándose en la información recabada del uso del reloj. veamos algunos comandos interesantes:

- `C-c C-x C-r` : Inserta un bloqueo dinámico, manteniendo una tabla sobre el fichero actual, la cual es parcialmente actualizada cuando el cursor se encuentra encima de una tarea. A continuación se puede ver un ejemplo.

```
#+BEGIN: clocktable :maxlevel 2 :scope subtree
Clock summary at [2012-09-12 mié 00:07]

| Headline     | Time   |
|--------------+--------|
| *Total time* | *0:00* |
#+END:
```

Para crear una tabla con las diferentes tareas y el tiempo dedicado:

```
#+begin: clocktable :maxlevel 5 :scope file :block today-1 :indent
#+END:
```

Los parámetros que acepta clocktable pueden consultarse aquí.

Finalmente, si se desea establecer parámetros de esfuerzo realizado para mejorar o ver en que tareas se dedica la mayor cantidad de tiempo, se debe de emplear la propiedad *Effort*. Para ello se dispone de los siguientes keystrokes:

- `C-c C-x e` : Activa la propiedad 'Effort' para la entrada actual.
- `C-c C-x C-e` : Modifica la estimación de esfuerzo del item actual que es cronometrado.

Un ejemplo podria ser:

```
#+PROPERTY: Effort_ALL 0 0:10 0:30 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00
#+COLUMNS: %40ITEM(Task) %17Effort(Estimated Effort){:} %CLOCKSUM
```

- Agenda

  Emacs integra las funciones de un calendario de escritorio, y Org-mode la explota con una agenda de eventos planificados y pasados, así como el estado de las tareas (TODO) y headlines. Además tiene facilidades para manejar citas, y registrar cuánto tiempo ha estado trabajando en uno o más proyectos o tareas. Por esta razón, Org facilita en modo de vistas el disponer de una visión del estado de las tareas, o de eventos que son importantes en fechas concretas.

  El calendario ocupa su propio buffer, cuyo modo principal es el modo Calendar. El caso de la agenda es similar, con la particularidad de que se trata de un buffer de sólo lectura. Sin embargo,

existen comandos que generan vistas sobre las localizaciones correspondientes en los ficheros Org originales, e incluso permiten editar estos ficheros remotamente. La edición remota desde los buffer de agenda permite modificar las fechas de reuniones y citas desde el buffer de agenda.

Los ficheros de agenda se deben de identificar como tales, ya sea mediante keystrokes (`C-c [`) o configurándolos en el fichero *.emacs* en la variable *org-agenda-files*. Es a partir de dichos ficheros de donde se extrae la información.

Para acceder a la agenda se utiliza el keystroke básico `C-c a` y seleccionar la vista de agenda que se quiere acceder pulsando:

- `a` : Presenta una agenda mostrando la planificación de las tareas a realizar durante la semana.
- `t/T` : Muestra una lista global de todos los TODO de todos los archivos de agenda en un solo buffer. Además, es posible modificar los mismos.
- `m/M` : Muestra una lista de marcas o propiedades en forma de headlines con parámetros coincidentes con una expresión lógica booleana que haga referencia a los TAGS buscados. Por ejemplo 'WAITING|CANCEL'.
- `L` : Muestra una vista de la línea de tiempo para el buffer actual. El objetivo es disponer de una vista general a través de eventos en un proyecto.
- `s` : Muestra una lista de entradas seleccionadas por una expresión booleana de palabras clave o expresiones regulares que debe, o no debe, ocurrir en la entrada. Muy útil a la hora de localizar notas.

Las posibilidades de la agenda son muchas, sobretodo si se personaliza su utilización. Sin embargo, esto vas más allá del alcance de este proyecto fin de carrera.

Extensiones de ORG

He comentado en reiteradas ocasiones la potencia de Emacs, y en parte se debe a su capacidad de instalar extensiones. Emacs dispone de un administrador de extensiones llamado *package.el*. Es un administrador que posee funcionalidades similares a *apt* en Debian, *YUM* en Red Hat o openSUSE, si bien mucho más limitado.
Esta extensión es capaz de manejar múltiples repositorios de extensiones, y permite buscar, instalar, actualizar y eliminar paquetes de Emacs. La función *list-packages* muestra los paquetes de los repositorios especificados en la configuración o ELPS por defecto. Para definir los repositorios, se agrega en el archivo *.emacs* (o el archivo utilizado para inicializar) de la siguiente forma:

```
(setq package-archives '(('gnu' . 'http://elpa.gnu.org/packages/')
                         ('marmalade' . 'http://marmalade-repo.org/packages/')
                         ('melpa' . 'http://melpa.milkbox.net/packages/')))
```

Una vez ejecutada la función de listar paquetes, se listan en un buffer todos los paquetes disponibles y los instalados. Al hacer click o seleccionar un determinado paquete, éste será marcado para su instalación. Una vez marcado, se presiona 'x' y Emacs preguntará si desea efectuar los cambios marcados. Al responde afirmativamente se iniciará la instalación. Hay otros comandos interesantes como 'd' (delete) para eliminar, y 'U' (update), para marcar todos los paquetes que se pueden actualizar a versiones más recientes.
Otra alternativa para instalar un paquete es ejecutar directamente la función *package-install* y escribir el nombre del paquete a ser instalado. Sin embargo, es más intuitivo utilizar *list-packages*, ya que permite buscar en el buffer con `C-s` sobre el buffer de texto de solo lectura. Adicionalmente, me muestra una descripción y el estado de los paquetes, incluyendo algunos marcados como nuevos.

Cifrado de información

Algo que debería de ser una máxima cuando se trabaja en un proyecto en el que hay diferentes intereses, datos sensibles, y en general, información que no debe de ser fácilmente accesible, es trabajar en un entono seguro. Para ello, la información debería de guardare en volúmenes cifrados, y, dado que dichos volúmenes van a estar accesibles durante mucho tiempo facilitando el acceso a nuestra información (que está en texto plano), dicha información debería de cifrarse individualmente. La política de contraseñas queda del lado de la responsabilidad de cada uno.
EasyPG es una funcionalidad incluida dentro del paquete Emacs que permite utilizar funcionalidades de GPG (GnuPG). Está integrado por defecto en las últimas versiones, pero, si no está instalado, sólo hay que incluir en nuestro fichero de configuración (por ejemplo =/.emacs) la siguiente configuración:

```
;; EasyPG (GPG for emacs)
(require 'epa)
(require 'epa-file)
(epa-file-enable)

; EPG support for GNUS
(setq gnus-treat-x-pgp-sig t
mm-verify-option 'always
mm-decrypt-option 'always)
```

Lo primero que debemos de hacer, para no limitar el cifrado a la utilización de contraseñas simétricas, es generar nuestro par de claves privada y publica, o bien importar claves de algún repositorio o servidor de claves para poder cifrar documentos que luego enviaremos a algún receptor.
Tenemos 3 formas básicas de cifrar un archivo:

1. Cifrar desde la consola utilizando comandos *gpg*.

   ```
   gpg -armor -recipient CLAVEID -encrypt fichero_a_cifrar
   gpg -armor -output fichero_cifrado -recipient CLAVEID -encrypt fichero_a_cifrar
   ```

   Donde la opción *–armor* cifra el fichero original y el archivo de salida se obtiene en formato ASCII. En caso de que no se especifique dicha opción, el fichero de salida sera un fichero binario.

2. Editar un buffer con extensión *.gpg*. Al guardar el buffer en un fichero Emacs, este solicitará que se seleccione, utilizando la letra 'm', alguna de las claves disponibles. En el caso de que no se seleccione ninguna clave, se solicitara una clave simétrica para cifrar el archivo. Una vez seleccionado el mensaje sera cifrado. Si salimos de emacs veremos que desde consola el fichero 'es ilegible', es decir, esta cifrado. Si abrimos esta vez el fichero .gpg con emacs nos pedirá la contraseña simétrica o la que se requiera para utilizar la clave privada y, de este modo, poder descifrarlo, haciendo éste legible otra vez.

3. Podemos, desde Emacs, seleccionar una región de un buffer (o el buffer completo) y ejecutar la secuencia `M-x epa-encrypt-region`. Para descifrar realizaremos el mismo proceso de seleccionar una región cifrada y presionando `M-x epa-decrypt-region`.

   Un ejemplo práctico sería:

   - Texto claro:

- Texto cifrado:

```
   -----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.14 (GNU/Linux)

jA0EAwMCbX0Vkdy7ZyZgyT8/XhthZKTi4+/vXzMmimLv4OB9nNHjUBKES9/EVjIM
uYH6WC0PJbAjgs6Acg1VgYpcgWm6G85JQmCYTuSFNts=
=RbX4
-----END PGP MESSAGE-----
```

- Clave de cifrado: PFC

Una práctica recomendable es asociar a dichas funciones algún keystroke para acelerar dicho proceso si lo hacemos de forma habitual. Para asociar las teclas 'C-c i" para cifrar una región y 'C-c o" para descifrarla, se debe de añadir :

```
;; To cipher a region
;; M-x epa-encrypt-region OR
(global-set-key (kbd 'C-c i') 'epa-encrypt-region)
;; To uncipher a region
;; M-x epa-decrypt-region OR
(global-set-key (kbd 'C-c o') 'epa-decrypt-region)
```

Bloques de código

Bueno, bueno, bueno. Dado que uno de los temas que vamos a tratar de hacer es ejecutar desde Emacs el máximo número de pruebas, uno de los aspectos que hay que conocer es cómo ejecuto comandos o código desde Emacs.
Los keystrokes que hay que conocer son básicamente:

- `<s {TAB}` : Para crear el contexto inicial donde se desarrolla el trozo (snippet) de código en el lenguaje seleccionado dentro de los posibles. El boque de código se compone de:

  ```
  #+NAME: <nombre>
  #+BEGIN_SRC <lenguaje> <switches> <argumentos>
    <cuerpo>
  #+END_SRC
  ```

  El hecho de nombrar el bloque de código, permite que éste sea evaluado desde otros puntos del fichero actual o de otros.

  El lenguaje indica el lenguaje del código utilizado en el bloque.

  Los switches son parámetros opcionales que permiten controlar aspectos de la exportación del bloque de código.

  Los argumentos, que pueden establecerse a nivel de bloque de código, o mediante propiedades, a nivel de buffer o árbol, permiten controlar muchos aspectos de la evaluación, exportación y tangling de los bloques de código.

  El cuerpo como tal, es el código fuente específico en el lenguaje especificado.

- `C-c C-C` : Para ejecutar el trozo de código.

Por ejemplo, para ejecutar en la shell una serie de comandos, se expresará en el formato en el que aparece el siguiente ejemplo. Una vez se ejecute, los resultados aparecen a continuación de `#+RESULTS:`.

```
#+BEGIN_SRC sh :exports both
  cd =/org
  wc -l charla.org
  ls -l charla.org | awk '{print $1,$5}'
#+END_SRC

 #+RESULTS:
|        128 | charla.org |
| -rw-rw-r-- |       3689 |
```

Otros bloques de código, ya sean ejemplos, código LaTeX, HTML, etc siguen la misma forma de uso. Pulsamos '<' seguido de una de las opciones del listado que vemos a continuación y pulsar `<TAB>`, por ejemplo '<e' y presionar `<TAB>`

- s #+BEGIN_SRC ... #+END_SRC
- e #+BEGIN_EXAMPLE ... #+END_EXAMPLE
- q #+BEGIN_QUOTE ... #+END_QUOTE
- v #+BEGIN_VERSE ... #+END_VERSE
- c #+BEGIN_CENTER ... #+END_CENTER
- l #+BEGIN_\LaTeX{} ... #+END_\LaTeX{}
- L #+LaTeX:
- h #+BEGIN_HTML ... #+END_HTML
- H #+HTML:
- a #+BEGIN_ASCII ... #+END_ASCII
- A #+ASCII:
- i #+INDEX: line
- I #+INCLUDE: line

Se pueden instalar nuevos templates customizando la variable *–org-structure-template-alist–*.
Otra forma de ejecutar un comando es directamente desde un enlace. La sintaxis es la misma que ya se ha visto en los enlaces]], pero se introduce el concepto *shell* en el *objetivo* seguido del comando a ejecutar.

```
[[shell:okular -p 37 documento.pdf &][documento.pdf página 37]]
```

Exportar a

Si bien es cierto que nuestro editor, junto con Org-mode, permite crear archivos de texto aparentemente sin marcado, o con pocos aspectos de marcado, éste dispone de la posibilidad de exportar el texto a múltiples formatos.
No es objetivo de este proyecto adentrarnos en todas y cada una de las posibilidades que tenemos. Por defecto es posible exportar a:

- ascii (ASCII format)
- beamer (LaTeX Beamer format)
- html (HTML format)
- icalendar (iCalendar format)
- latex (LaTeX format)
- man (Man page format)
- md (Markdown format)
- odt (OpenDocument Text format)
- org (Org format)
- texinfo (Texinfo format)

En este caso con un sólo keystroke es suficiente para iniciar el proceso de exportación.

- `C-c C-e` Para seleccionar el formato de exportación en función del listado de opciones para la exportación.

Es importante disponer de un marco de variables (export keywords) adecuadas al formato y el objetivo de la exportación del archivo. Cada una de estas palabras claves se corresponde con una variable global. El actual documento configura las siguientes palabras clave:

```
#+TITLE: Emacs
#+OPTIONS:  H:3 num:nil toc:t \n:nil @:t t |:t ^:t -:t f:t *:t
#+OPTIONS:  TeX:t LaTeX:t skip:nil d:(HIDE) tags:not-in-toc todo:nil
#+STARTUP:  align fold nodlcheck hidestars oddeven lognotestate overview
#+TAGS:     Actual (a) Mejorar(m) noexport(n)
#+SEQ_TODO: TODO(t) INPROGRESS(i) WAITING(w@) | DONE(d) CANCELED(c@)
#+AUTHOR:   José Luis Jerez Guerero
#+EMAIL:    jljerez AT error0x01 DOT net
#+LANGUAGE: es
#+CATEGORY: PFC
```

Es particularmente interesante la exportación a LaTeX a la hora de desarrollar los informes. Es por esa razón que recomiendo la lectura y comprensión de los diferentes atributos específicos que se pueden utilizar para mejorar la presentación de los mismos.